UNDERSTANDING STUDENT PERSPECTIVE OF UNDERGRADUATE CYBERSECURITY PROGRAMS AND EXPERIENCES ACROSS CHRISTIAN COLLEGES AND UNIVERSITIES

A Prospectus Presented in Partial Fulfillment Of the Requirements for the Degree Doctor of Education by Brandon P. Grech

Liberty University, Lynchburg, VA

2022
UNDERSTANDING STUDENT PERSPECTIVE OF UNDERGRADUATE
CYBERSECURITY PROGRAMS AND EXPERIENCES ACROSS
CHRISTIAN COLLEGES AND UNIVERSITIES

by Brandon P. Grech

A Prospectus Presented in Partial Fulfillment
Of the Requirements for the Degree
Doctor of Education

Liberty University, Lynchburg, VA

02/22/2022

APPROVED BY:
ABSTRACT

The number of Christian colleges and universities that are offering cybersecurity four-year degrees is rising. The workforce is in dire need of cybersecurity professionals; however, has anybody asked the new cybersecurity professionals in the workforce how their recent academic experience prepared them for such a global need? Research is well-documented about what industry currently needs in cybersecurity professionals; however, this research focused on asking graduates what students need for the workforce. The purpose of this explorative qualitative study was to gain an understanding of the phenomena of the holistic experience (technical, non-technical, and whole-person) strengths and shortcomings (if any) recent cybersecurity graduates who are now in the workforce experienced at various Christian colleges and universities during their undergraduate education. The population of this research was recent graduates of Christian undergraduate cybersecurity programs that are currently in the cybersecurity workforce. The gap that drove this study was the need to learn how current cybersecurity programs have influenced and molded students for the workforce and allow Christian cybersecurity program leaders to utilize this research and optimize the experience their students have at their institution. The theory which guided this exploratory research was academic outcomes assessment theory in which student opinions are sought to identify the satisfaction relationship their technical, non-technical, and whole-person development in their Christian undergraduate program as preparation for real-world application. This qualitative, exploratory, phenomenological research identified Christian undergraduate program strengths and gaps, such as an overwhelming trend of recent cybersecurity graduates that are not fully satisfied with their technical development.

Keywords: cybersecurity, development, curriculum, undergraduate, education.
Dedication

This work and all previous work that led to the creation of this research are dedicated to each of the following.

First and foremost, I thank my Lord and Savior Jesus Christ for blessing me with every breath on this earth, every loved one He has placed in my life, and giving me the capabilities and resources to perform work in Christian cybersecurity education to advance the Kingdom of God. Please bless me with wisdom, guidance, strength, and time to do your will, Lord.

To my wife, best friend, and mother of our children, Sarah. Thank you for supporting me in both my career endeavors during the day and academic endeavors during the evenings and weekends. The last ten years of sacrifice you have selflessly given to allow me to grow and learn personally, professionally, and spiritually has been a gift I will forever be grateful for. I would not have been able to do any of this without you. I cannot imagine spending this earthly life without you. Thank you for always challenging me to continue becoming the man I’m supposed to be. I’m trying. I love you.

To my daughters, Jennifer and Jane. Thank you for the joy and happiness you bless me with every day. Thank you for being patient with me and allowing me to spend time away from you to complete this academic journey. I encourage you all to continue to grow in the Lord and learn from your godly mother. We are all extremely blessed to have such a wonderful woman in our lives. I love you girls.

To my unborn son, who may be born any day. I look forward to getting to know you and sharing with you the stories our family has experienced over the last ten years. I am thankful to have completed this academic journey before your arrival; however, please
know it would not have been possible without your mother and sisters. Please learn from them, especially your godly mother. They love you. I love you also son.

To my parents, John and Michelle. Thank you for your love and support during my childhood. Thank you for placing me in wonderful Christian environments throughout my childhood to grow in the Lord and learn from others. Jennifer, Jane, and our unborn son are blessed to have you both as grandparents.

To my in-laws, Jacob and Marjorie. Thank you for allowing me to marry your daughter and being so supportive of Sarah’s and my journey throughout our first ten years of marriage. Jennifer, Jane, and our unborn son are blessed to also have you both as grandparents.

To my fellow Airmen that I served alongside. Thank you for supporting me and encouraging me during my military career, academic pursuits, and leadership development. Thank you for blessing me with such wonderful opportunities. You all helped mold me and prepare me for this work.

In memory of my grandmother, Suzanne E. Smith. Thank you for the never-ending love and grace you showed me as a child. Grace, love, and peace were among the qualities I witnessed you share amongst all of your children, grandchildren, and loved ones. You showed us all how to live a life in accordance with Galatians 5:22-23. You are forever missed here; however, we know you are at home with the Lord.

In memory of my first boss and mentor, Rev. Robert Henry. Thank you for spending so much time with me as an adolescent. Thank you for showing me the meaning of dedication and hard work. Thank you for being a man of God the entire community looked up to. Your spirit, jokes, words, and actions left such a positive impact on the Kingdom of
God and the Falls Creek community that I cannot measure. I would be remiss if I did not also thank Rev. Robert Henry’s surviving wife, Jeanne Henry. Thank you for your ministry through music and for allowing your husband to spend so much time with me during those years. It made a lifelong impact on me.
Acknowledgments

Besides the loved ones mentioned above, I would also like to specifically acknowledge, Dr. Gary J. Bredfeldt, Dr. Steve Yates, and the entire Christian Leadership program at the Rawlings School of Divinity at Liberty University. Thank you for your guidance during this research and for allowing me to learn from you all.

I would also like to specifically acknowledge Dr. Kenneth J. Knapp for allowing me to spend my career dedicated to helping our Anderson University (SC) cybersecurity students grow in the Lord and the field of cybersecurity. Thank you for supporting this research and giving me the capabilities and resources to do this work that I truly love.

I would also like to acknowledge all of my current and future Anderson University (SC) cybersecurity students and their supportive families and friends. Thank you for entrusting me with your development. My career is dedicated to helping get you where you want to go personally, professionally, and spiritually. I truly have the best job and I never let that go for granted.

I would also like to acknowledge all of my friends and mentors I had throughout my earthly journey at the following organizations:

- Beechwoods Presbyterian Church, Falls Creek, PA
- DuBois Christian Schools, DuBois, PA
- United States Air Force
- University of Maryland Global Campus, Adelphi, MD
- Bay Ridge Christian Church, Annapolis, MD
- National University, San Diego, CA
- Carnegie Mellon University, Pittsburgh, PA
- Trinity Point Church of God, Clarion, PA
- Anderson University, Anderson, SC

Finally, I would like to thank the seven anonymous participants that partook in this research. I cannot disclose your names for anonymity purposes; however, please know that
this work would have been impossible without your willingness to help a researcher you did not personally know. Your time and responses will help shape the experiences of current and future cybersecurity students at Christian institutions.
# Table of Contents

ABSTRACT ............................................................................................................................... 3

Copyright .................................................................................................................................... 4

Dedication ................................................................................................................................... 5

Acknowledgments ....................................................................................................................... 8

List of Tables ............................................................................................................................ 14

List of Figures ........................................................................................................................... 17

List of Abbreviations ................................................................................................................. 18

CHAPTER ONE: RESEARCH CONCERN .............................................................................. 22

  Introduction ................................................................................................................ 22

  Background to the Problem ...................................................................................... 22

  Statement of the Problem ......................................................................................... 24

  Purpose Statement....................................................................................................... 25

  Research Questions ....................................................................................................... 26

  Assumptions and Delimitations ..................................................................................... 27

    Research Assumptions ................................................................................................. 27

    Delimitations of the Research Design ......................................................................... 27

  Definition of Terms ....................................................................................................... 28

  Significance of the Study ............................................................................................... 30

  Summary of the Design ................................................................................................. 30

CHAPTER TWO: LITERATURE REVIEW ............................................................................. 31

  Overview ....................................................................................................................... 31

  Theological Framework for the Study ........................................................................... 31
Theoretical Framework for the Study ................................................................. 39
Related Literature ................................................................................................. 54
  Rationale for the Current Study ........................................................................ 54
  Identified Gap in the Literature ....................................................................... 68
Profile of the Current Study .................................................................................. 69
CHAPTER THREE: RESEARCH METHODOLOGY .................................................. 70
Research Design Synopsis ................................................................................... 70
  The Problem ...................................................................................................... 70
  Purpose Statement ........................................................................................... 71
  Research Questions ......................................................................................... 73
  Research Design and Methodology ................................................................. 73
Setting .................................................................................................................. 74
Participants .......................................................................................................... 77
Role of the Researcher ......................................................................................... 78
Ethical Considerations ......................................................................................... 80
Data Collection Methods and Instruments ......................................................... 81
  Collection Methods ....................................................................................... 81
  Instruments and Protocols ............................................................................. 82
  Procedures ..................................................................................................... 84
Data Analysis ....................................................................................................... 87
  Analysis Methods ......................................................................................... 87
  Trustworthiness ............................................................................................ 89
Chapter Summary ............................................................................................... 92
List of Tables

Table 1: Taxonomy of Specialty Area ................................................................. 57
Table 2: CSEC 2017 Model of Cybersecurity ...................................................... 58
Table 3: Courses for Cybersecurity Certificate at UMSL ................................. 61
Table 4: Integrating Certification Material into Undergraduate Courses Matrix ... 64
Table 5: Participants' Institution ....................................................................... 100
Table 6: Participants' Degree ............................................................................ 100
Table 7: Participants' Graduation Year ............................................................... 101
Table 8: Participants' Time in Workforce ......................................................... 101
Table 9: Participants' Current Work ................................................................. 102
Table 10: Participants' Work Role Satisfaction .................................................. 103
Table 11: Overall Technical Satisfaction ........................................................... 104
Table 12: Overall Technical Satisfaction Detailed ............................................ 105
Table 13: Technical Knowledge or Skills ......................................................... 106
Table 14: Technical Strengths .......................................................................... 107
Table 15: Technical Gaps ................................................................................ 108
Table 16: Technical Satisfaction Related to Work Role ..................................... 109
Table 17: Technical Satisfaction Related to Work Role Detailed ....................... 109
Table 18: Technical Knowledge or Skills Related to Work Role ....................... 110
Table 19: Technical Strengths Related to Work Role ....................................... 111
Table 20: Technical Gaps Related to Work Role .............................................. 112
Table 21: Technical Recommendations Experienced ....................................... 113
Table 22: Technical Recommendations Not Experienced ............................... 114
Table 23: Additional Technical Strengths and/or Gaps Experienced ........................................ 115
Table 24: Overall Non-Technical Satisfaction ......................................................................... 116
Table 25: Overall Non-Technical Satisfaction Detailed ........................................................... 117
Table 26: Non-Technical Knowledge or Skills ........................................................................ 118
Table 27: Non-Technical Strengths ......................................................................................... 118
Table 28: Non-Technical Gaps ................................................................................................ 119
Table 29: Non-Technical Satisfaction Related to Work Role ................................................... 120
Table 30: Non-Technical Satisfaction Related to Work Role Detailed ..................................... 121
Table 31: Non-Technical Knowledge or Skills Related to Work Role ..................................... 122
Table 32: Non-Technical Strengths Related to Work Role ....................................................... 122
Table 33: Non-Technical Gaps Related to Work Role ............................................................. 123
Table 34: Non-Technical Recommendations Experienced ....................................................... 124
Table 35: Non-Technical Recommendations Not Experienced ................................................ 125
Table 36: Additional Non-Technical Strengths and/or Gaps Experienced ................................ 126
Table 37: Overall Whole-Person Satisfaction .......................................................................... 127
Table 38: Overall Whole-Person Satisfaction Detailed ............................................................ 127
Table 39: Whole-Person Development Time ........................................................................... 128
Table 40: Whole-Person Strengths .......................................................................................... 129
Table 41: Whole-Person Gaps ................................................................................................. 130
Table 42: Whole-Person Satisfaction Related to Work Role .................................................... 131
Table 43: Whole-Person Satisfaction Related to Work Role Detailed ...................................... 131
Table 44: Whole-Person Development Time Related to Work Role ......................................... 132
Table 45: Whole-Person Strengths Related to Work Role ........................................................ 133
Table 46: Whole-Person Gaps Related to Work Role .............................................................. 134
Table 47: Whole-Person Recommendations Experienced ................................................... 134
Table 48: Whole-Person Recommendations Not Experienced ......................................... 135
Table 49: Whole-Person Biblical Traits Strengths or Weaknesses ................................... 136
Table 50: Additional Whole-Person Strengths and/or Gaps Experienced ......................... 137
Table 51: Cumulative Undergraduate Experience Essay ................................................... 139
Table 52: Time Taken in Survey (Least to Greatest).......................................................... 141
List of Figures

Figure 1: Christen et al.'s First Draft of a Map on Value Conflicts in Cybersecurity ..............47
Figure 2: Process of Decrypting Encrypted HTTPS Traffic to Cleartext HTTP Traffic ..........49
Figure 3: NetworkMiner Example of Decrypted HTTPS Traffic ..........................................49
Figure 4: CompTIA's IT Certification Roadmap .................................................................50
Figure 5: Jeopardy-style CTF Example with 1 Solved Challenge .......................................65
Figure 6: Creswell's Data Analysis Flow Chart .................................................................88
Figure 7: Sentiment Analysis of Overall Technical Satisfaction Detailed Responses ............105
Figure 8: Sentiment Analysis of Overall Non-Technical Satisfaction Detailed Responses ....117
Figure 9: Sentiment Analysis of Overall Whole-Person Satisfaction Detailed Responses ....128
Figure 10: Sentiment Analysis of Cumulative Undergraduate Experience Essay ...............141
Figure 11: Time Taken in Survey (Order of Participation) ................................................142
List of Abbreviations

Accreditation Board for Engineering and Technology (ABET)

Amazon Web Services (AWS)

Capture The Flag (CTF)

Center of Academic Excellence – Cyber Defense (CAE-CD)

Center of Academic Excellence – Cyber Defense Education (CAE-CDE)

Center of Academic Excellence – Cyber Operations (CAE-CO)

Center of Academic Excellence – Information Assurance Education (CAE-IAE)

Center of Academic Excellence – Research (CAE-R)

Center of Academic Excellence (CAE)

Certified Cloud Security Professional (CCSP)

Certified Ethical Hacker (CEH)

Certified Expert Practitioner (CEP)

Certified Information Systems Security Professional (CISSP)

Chief Information Security Officer (CISO)

Collegiate Cyber Defense Competition (CCDC)

Common Vulnerabilities and Exposures (CVE)

Common Vulnerability Scoring System (CVSS)

CompTIA Advanced Security Practitioner (CASP+)

CompTIA Cybersecurity Analyst (CySA+)

Computer Emergency Response Team (CERT)

Computer Science (CMP SCI)

Computing Sciences Accreditation Board (CSAB)
Council for Christian Colleges & Universities (CCCU)
Cybersecurity and Infrastructure Security Agency (CISA)
Cybersecurity Awareness Worldwide (CSAW)
Cybersecurity Curricular Guideline (CSEC 2017)
Demilitarized Zone (DMZ)
Department of Defense (DoD)
Department of Homeland Security (DHS)
Enterprise Service Group (ESG)
Enterprise Strategy Group (ESG)
Federal Virtual Training Environment (FedVTE)
Global Information Assurance Certification (GIAC)
Governance, Risk Management, and Compliance (GRC)
Group Policy Objects (GPOs)
Hypertext Transfer Protocol (HTTP)
Hypertext Transfer Protocol Secure (HTTPS)
Information Assurance (IA)
Information Systems (INFSYS)
Information Systems Security Association (ISSA)
Information Technology (IT)
Institute of Electrical and Electronics Engineers (IEEE)
Institution of Higher Education (IHE)
Institutional Review Board (IRB)
International Capture The Flag (iCTF)
International Information System Security Certification Consortium ((ISC)²)

International Sports Sciences Association (ISSA)

Internet of Things (IoT)

Intrusion Detection System (IDS)

Intrusion Prevention System (IPS)

Knowledge Units (KUs)

Knowledge, Skills, and Abilities (KSA)

Licensed Penetration Tester (LPT)

Malware Information Sharing Platform (MISP)

Multi-Factor Authentication (MFA)

National Initiative for Cybersecurity Education (NICE)

National Institute of Standards and Technology (NIST)

National Nuclear Security Administration (NNSA)

National Security Agency (NSA)

National Security Agency Center of Academic Excellence (NSA/CAE)

New International Version (NIV)

Offensive Security Certified Professional (OSCP)

Open-Source Intelligence (OSINT)

Open-source software (OSS)

Resident Director (RD)

Risk Management Framework (RMF)

Scholarship for Service (SFS)

Security Information and Event Management (SIEM)
Security Operation Center (SOC)

Single Sign-On (SSO)

Software Engineering Institute (SEI)

South Carolina (SC)

Specialty Area (SA)

Technology, Entertainment, Design (TED)

Transport Layer Security (TLS)

University of Missouri-St. Louis (UMSL)

United States (US)
CHAPTER ONE: RESEARCH CONCERN

Introduction

The purpose of this qualitative, exploratory, phenomenological research was to gain an understanding of the perspectives of recent Christian college and university cybersecurity graduates regarding the holistic experience (technical, non-technical, and whole-person) strengths and shortcomings (if any) of their undergraduate academic program as preparation for the workforce. The number and complexity of cyberattacks, such as ransomware and web application attacks, continue to rise (Verizon, 2020). This increase has led to 500,000+ current U.S.-based cybersecurity job openings while ~940,000 U.S.-based cybersecurity workers currently exist (Cyber Seek, 2021). This severe workforce need continues to be a sector of opportunity for colleges and universities to create a cybersecurity program to meet this market.

As a Christ-centered institution of higher education is centered on unchanging biblical doctrine, how can the ever-changing cybersecurity workforce requirements be met by Christian colleges and universities? For this research, the researcher was interested in understanding the impact faculty members of Christian colleges are having when creating their cybersecurity curriculum, program, and overall experience from the viewpoint of the student and eventual graduate. Does the theological Christian belief and mission of the institution alter, in any way, the satisfaction of students regarding their cybersecurity education? What strengths or gaps exist, if any, within Christian cybersecurity baccalaureate degree education?

Background to the Problem

The growth of cybersecurity undergraduate programs continues to rise amongst Christian colleges and universities. Currently, the need for cybersecurity professionals is so large that every graduate that seeks a job will find one (as there is a zero percent unemployment rate)
(Schwartz, 2019). This need for businesses to hire cybersecurity professionals leaves higher education institutions vulnerable to not identifying gaps in the holistic development the students experience during their undergraduate timeframe as each of their students is being hired. There is a need to research the effectiveness of Christian cybersecurity programs as perceived by recent graduates that are now in the workforce.

A shortage in the global cybersecurity workforce continues to be a problem for companies in all industries and of all sizes. This shortage remains the number one job concern for those working in the field. That is not surprising given that 2018 was “the year of the megabreach” ((ISC)², 2019, p. 3). Municipalities are getting hit hard by ransomware, and mobile malware attacks have doubled (p. 3). The cybersecurity workforce gap has continued to increase, primarily due to a global surge in hiring demand. In the U.S., the cybersecurity workforce gap is nearly 500,000. By combining our U.S. cybersecurity workforce estimates and this gap data, we can calculate that the cybersecurity workforce needs to grow by 62% in order to meet the demands of U.S. businesses today. Using the workforce estimate of 2.8 million based on the 11 economies for which we provided a workforce estimate and the global gap estimate of 4.07 million, we can estimate that the global workforce needs to grow by 145% (p. 8). The Council for Christian Colleges & Universities (CCCU) (as of January 20, 2022) includes over 150 institutions in the United States. Out of these institutions, only three of the Christian colleges and universities are listed as Center of Academic Excellence (CAE) in Cyber Defense by the National Security Agency (NSA). The NSA/CAE is intended to promote higher education and research in cyber defense and producing professionals with cyber defense expertise (NSA, 2020, p. 6). The three institutions that are listed as a National Center of Academic Excellence in Cyber Defense and a member of the CCCU are Montreat College, Regent University, and Oklahoma
Christian University. Some Christian colleges currently have cybersecurity programs that are not part of CCCU (e.g., Pensacola Christian College, Cedarville University, etc.); however, this is still an indicator of the minimal number of Christian institutions of higher education that are developing cybersecurity professionals.

Research over the last several years continues to agree that organizations are struggling to attain, attract, and retain cybersecurity professionals. According to (ISC)² (2019):

65% of organizations represented have a shortage of staff dedicated to cybersecurity. That lack of skilled/experienced cybersecurity personnel is the top concern among survey respondents—even more of a concern than a lack of resources to do their jobs effectively. In addition, 51% of cybersecurity professionals say their organization is at moderate or extreme risk due to cybersecurity staff shortage. (p. 9)

The path into cybersecurity is dynamic and not as clear as it may be for other careers. Different organizations require different education, certification, and experience of cybersecurity candidates. “Cybersecurity professionals are likely to have at least a bachelor’s degree—with a little more than one-third holding a master’s or doctoral/post-doctoral degree. While most in the field get their degrees in computer and information sciences (40%), others get degrees that are not IT-focused, such as engineering (19%) and business (10%)” ((ISC)², 2019, p. 14).

Statement of the Problem

Cybersecurity education at any level can vary greatly amongst different institutions. Institutions have the flexibility to solely or heavily focus on technical skills or choose to prioritize developing non-technical skills with the curriculum and program. Another difference seen amongst higher education institutions is whether or not the courses within the cybersecurity degree align with cybersecurity certifications. These cybersecurity certifications usually do not require a degree and can be attained without formal training. This lack of a requirement for a college degree to attain cybersecurity certifications causes a division of opinions on whether or
not certification-driven cybersecurity courses should be included within a cybersecurity program (Knapp et. al, 2017).

The challenge here is that over 300 colleges and universities have been approved by the rigorous criteria of the NSA/CAE (CAE Institution Map, 2021). Only three of the NSA/CAE programs are part of higher education institutions within the CCCU. Are Christian colleges that are offering cybersecurity bachelor’s degrees looking to eventually attain NSA/CAE accreditation, or are the colleges and universities creating a unique approach to delivering cybersecurity education?

The flexibility cybersecurity program directors and leaders have, while the market has a zero-percent unemployment rate, leaves these programs vulnerable to assuming their programs are meeting the needs of the students and the workforce when the workforce is starving for talent and all cybersecurity professionals are hired. Analyzing the effectiveness of these programs before either the demand for cybersecurity entry-level professionals drops, or companies decide against hiring cybersecurity professionals after their undergraduate journey is complete at certain institutions, will better protect current and future students within this four-year cybersecurity developmental pipeline to be optimally prepared for their place in the workforce.

Purpose Statement

The purpose of this qualitative, exploratory, phenomenological research was to gain an understanding of the perspectives of recent Christian college and university cybersecurity graduates regarding the holistic experience (technical, non-technical, and whole-person) strengths and shortcomings (if any) of their undergraduate academic program as preparation for the workforce. The categories the graduates utilized to describe their holistic undergraduate education are defined as technical, non-technical, and whole-person. The technical category
addressed technical cybersecurity topics (e.g., cryptography; networking; network defense; scripting; hacking; etc.). The non-technical category collected data pertinent to their preparation to perform non-technical cybersecurity topics (e.g., cybersecurity planning and management; policy, legal, ethics, and compliance; security risk analysis; cyber threats; etc.). The whole-person category assessed the non-cybersecurity-related skills and traits they developed at their institution (e.g., love; strength; steadfastness; faithfulness; being on guard; etc.).

The gap driving this study is the need to learn how current cybersecurity programs have influenced and molded students for the workforce and allow Christian cybersecurity program leaders to utilize this research and optimize the experience their students have at their institution.

The theory guiding this exploratory research is academic outcomes assessment theory in which student opinions are sought to identify the satisfaction relationship their technical, non-technical, and whole-person development in their Christian undergraduate program as preparation for real-world application.

**Research Questions**

**RQ1.** How would a recent graduate describe, if any, technical skill strengths and gaps commonly experienced in Christian cybersecurity undergraduate programs?

**RQ2.** How would a recent graduate describe, if any, non-technical skill strengths and gaps commonly experienced in Christian cybersecurity undergraduate programs?

**RQ3.** How would a recent graduate describe, if any, whole-person skill strengths and gaps commonly experienced in Christian cybersecurity undergraduate programs?

**RQ4.** How would a recent graduate describe their cumulative experience at a Christian cybersecurity undergraduate program?
Assumptions and Delimitations

Research Assumptions

This research assumed the definitions and sub-categories of technical and non-technical Knowledge Units (KUs) of the National Security Agency’s Center of Academic Excellence (NSA/CAE) are accurate. Furthermore, this research assumed that all cybersecurity workforce needs are in some capacity referenced in these documents. This research only utilized questions and areas in need that are based on the KUs.

This research also assumed that each Christian institution that has a cybersecurity undergraduate program that was surveyed in this research not only seeks to provide necessary technical and non-technical knowledge and skills related to cybersecurity but to also develop the whole-person.

Delimitations of the Research Design

1. This research is delimited to only private colleges that are members of the Council for Christian Colleges & Universities (CCCU), recognized as a Creation College by Answers in Genesis, and/or a Protestant Christian institution by viewing their website and/or mission/faith statement(s). It does not include public institutions, nor private and/or non-Protestant Christian religious institutions (including Catholic institutions).

2. The institution must have a brick-and-mortar presence and be headquartered in the United States of America. It does not include institutions that are based in a territory of the United States of America nor outside of the United States of America.

3. The participants must have graduated with a four-year degree in cybersecurity (or similar field, e.g., information security, computer security, etc.) from a Christian institution that meets the above requirements. It, therefore, excludes computer science and other technology and/or computer-centric degrees where the term ‘security’ is not in the major. It also excludes minors in cybersecurity (or a similar field) when the major does not meet the above requirement.

4. The participants have been employed full-time in the cybersecurity workforce no more than five full years after graduation and are currently employed in a cybersecurity role. This cybersecurity role can be filled anywhere. It, therefore, excludes students that have chosen to attend graduate school and do not work full-time in the cybersecurity workforce.
Definition of Terms

Within this study the following terms will adhere to these definitions:

1. **CompTIA**: Non-profit organization that is popular with cybersecurity education and certification provider. Some of their most common cybersecurity-related certifications are: Security+ (network security), PenTest+ (ethical hacking), CySA+ (cybersecurity), and CASP+ (advanced cybersecurity) (CompTIA, n.d.).

2. **Council for Christian Colleges & Universities (CCCU)**: The Council for Christian Colleges & Universities is a higher education association of more than 185 Christian institutions around the world. With campuses across the globe, including more than 150 in the U.S. and Canada and more than 30 from an additional 19 countries, CCCU institutions are accredited, comprehensive colleges and universities whose missions are Christ-centered and rooted in the historic Christian faith. Most also have curricula rooted in the arts and sciences. The CCCU’s mission is to advance the cause of Christ-centered higher education and to help our institutions transform lives by faithfully relating scholarship and service to biblical truth (Council for Christian Colleges & Universities, n.d.).

3. **Cyber Threat**: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service (NIST, 2021).

4. **Cyberattack**: An attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information (NIST, 2021).

5. **Cybersecurity**: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. More simply, the ability to protect or defend the use of cyberspace from cyberattacks (NIST, 2021).

6. **Cyberspace**: Similar to land, air, and water, cyberspace is considered the terrain where digital and cyberattacks occur. It is a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (NIST, 2021).

7. **International Information System Security Certification Consortium (Commonly referred to as (ISC)²)**: A non-profit organization that provides certification
opportunities and is a leader in cybersecurity surveys to identify current states of cybersecurity. “More than 140,000 certified members strong, we empower professionals who touch every aspect of information security” ((ISC)², n.d.).

8. National Institute of Standards and Technology (NIST): Non-regulatory federal agency that is tasked with creating a plethora of cybersecurity standards, regulations, research, and addressing the workforce shortage. Some of the resources that will be utilized are: CyberCorps Scholarship for Service (SFS); National Centers of Academic Excellence (CAE); and National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.

9. Non-technical skills: Regarding cybersecurity, a job role and skill that does not rely on the professional to be regularly working with the cybersecurity technology that is actively performing cybersecurity tasks. Some of these non-technical areas are: Cyber Threats; Policy, Legal, Ethics, and Compliance; Security Program Management; Security Risk Analysis; and Cybersecurity Planning and Management (NSA/CAE, 2020)

10. Recent graduate: A cybersecurity professional that has graduated from an undergraduate cybersecurity program from a Christian institution of higher education no more than five years ago and no less than three months ago.

11. Software Engineering Institute (SEI): A Federally Funded Research and Development Center located in Pittsburgh, Pennsylvania. The Software Engineering Institute is a part of Carnegie Mellon University, a top-tier research university. One of the divisions within the Software Engineering Institute is the CERT (Computer Emergency Response Team) Division. The Software Engineering Institute, with its ideal placement within the university, addresses challenges our nation faces. One of these issues is the cybersecurity workforce shortage. The SEI performs research of cybersecurity educational resources and methods for learning (Software Engineering Institute, n.d.).

12. Technical skills: Regarding cybersecurity, a job role and skill that primarily relies on the professional to be working directly with cybersecurity technology and have technical control over the information via information technology. Some of these technical areas are: Scripting and Programming, Networking, Network Defense, Cryptography; and Operating Systems Concepts (NSA/CAE, 2020).

13. Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source (NIST, 2021)

14. Whole-person skills: Any skill, education, or molding that is not primarily and/or directly related to cybersecurity, but growth as an adult.
Significance of the Study

This research surveyed students that graduated within the last five years regarding their satisfaction with the cybersecurity undergraduate holistic experience regarding technical, non-technical, and whole-person viewpoints. This research intended to better understand the process Christian institutions are preparing students for the workforce and the graduate’s satisfaction as not all cybersecurity programs follow NSA/CAE accreditation guidelines. The significance of this study was not to promote nor diminish the NSA/CAE, but to assess how satisfied graduates are regarding their preparedness after going through a four-year cybersecurity program at a Christian university regarding technical, non-technical, and whole-person development. The researcher looked for trends that speak positively and/or negatively regarding technical, non-technical, and/or whole-person development and if any conclusions can be determined to help enlighten current Christian cybersecurity program directors and leaders to self-assess if they see these strengths and/or weaknesses in their own institution and program.

Summary of the Design

This qualitative, exploratory, phenomenological research surveyed seven cybersecurity professionals that have graduated from a Christian undergraduate program within the last five years. This survey attempted to capture and analyze positive and negative trends that Christian cybersecurity programs have within their program and collegiate experience. Various research and references discuss the current skills cybersecurity professionals need to be successful in the workforce; however, this researcher is attempting to seek those who are experiencing the fruits of their academic rigor and labor. These individuals are in an optimal position to describe their recent educational experience while discussing how their holistic educational transformation either met or missed different aspects for their employment needs.
CHAPTER TWO: LITERATURE REVIEW

Overview

The recent rise of the demand for cybersecurity professionals has left institutes of higher education searching for methods to integrate cybersecurity program offerings to their students. This study will assess the current state of Christ-centered education environments for a non-theological and highly technical program that is cybersecurity. For this study to be supported, the literature review will have a theological framework referencing Christian education environment needs and the theoretical framework will reference cybersecurity educational needs and practices. Utilizing a dual-pronged approach will ensure that the study accurately defines best practices for Christian education as a whole (regardless of program) and cybersecurity education (regardless of religious beliefs of the institution). In other words, the final result of this research is grounded in Christ-centered education and be technically optimal.

Theological Framework for the Study

Roles of Christian Faculty

The framework of the roles of the Christian faculty member is based on Bredfeldt (2006) *Great Leader Great Teacher: Recovering the Biblical Vision for Leadership* and Knight (2006) *Philosophy & Education: An Introduction in Christian Perspective*. Understanding the various roles of Christian faculty members will allow those that are placed in non-theological faculty roles (e.g., technology) within a Christian institute of higher education to ensure their practice remains aligned with Christian theology.
Teaching the Word

A faculty member of a Christian institution of higher education must continuously study the Word and be able to teach the Word. When Christians think about those who are called to study the Word and teach the Word, they may be inclined to think about pastors and only pastors. The role of a Christian educator can also be categorized as a type of biblical leader thus allowing for additional roles and guidelines to be established. “Biblical leadership is taking the initiative to influence people to grow in holiness and to passionately promote the extension of God’s kingdom in the world” (Howell, 2003, p. 3). Without this foundational necessity of teaching the Word, there may not appear to be any difference between the instruction and lessons given to the students from a faculty member of a Christian institution and a faculty member of a non-Christian institution. “Since the function of Christian education is one of reconciliation and restoring the balanced image of God in students, education should be seen primarily as a redemptive act … the role of the teacher is ministerial and pastoral” (Knight, 2006, p. 198). Scripture is the foundation of providing a Christian worldview for the faculty member and the students through this means.

Luke 6:39-40 (NIV) discusses how the student, when fully trained, will be like their teacher. “He also told them this parable: “Can the blind lead the blind? Will they not both fall into a pit? The student is not above the teacher, but everyone who is fully trained will be like their teacher.” If the faculty member does not study the Word, treasure the Word, teach the Word, and live by the Word, then that will (sadly) be the result of the students. “The teaching authority of Scripture commits the believer at certain focal points and so provides an interpretive framework, an overall glimpse of how everything relates to God” (Holmes, 1987, p. 18).
Leading like Jesus

As the students, when fully trained, will be like their teacher, Christian education faculty members must continuously seek to be trained by Jesus. This ensures the faculty member can lead like Jesus (as they are students of Jesus Christ), thus ensuring that the students become like their teacher who is like Jesus. “The clearest and fullest integration of the gift of teacher-pastor is seen in the ministry of Christ … Christ may be seen as the best example of teaching in terms of methodology and meaningful interpersonal relations” (Knight, 2006, p. 216).

Learning from the Son of God that walked this earth around two thousand years ago is arguably best done by studying not only Scripture, but specifically the books Matthew, Mark, Luke, and John (known as the gospels). “(Studying the gospels) from the perspective of Christ as the teacher will contribute a great deal to our knowledge of how to operate in the classroom … direct contact with the aims and goals of Christian education” (Knight, 2006, p. 211). Ingram (2017) argues that studying the Word will highlight how the legacy of Christ is clearly seen due to performing perfect teaching and leadership training that forever changed this temporary world we currently live in. Ingram describes how Christ’s legacy is seen to this day through various means (e.g., being the dividing line in history where the calendar year is in reference to Him):

If it’s God’s desire for us to leave a legacy, it only makes sense that we would be able to see the practice modeled in Jesus’s ministry. We know about the legacy he left. Even unbelievers know about this one man who never traveled farther than sixty miles from his home and who had no mass media exposure. Eleven of his twelve closest followers were very committed, and a hundred and twenty others were more loosely committed. (pp. 253-254)

Utilizing the concept of teachers being like Christ so their students become like the teacher who is like Christ, is originally shown as Christ trained the disciples and the one hundred and twenty other believers referenced in Acts 1.
Jesus has a fourfold process of empowering great people that stands out clearly in the gospels. He brought them in, built them up, trained them for action, and sent them out. His disciples were ordinary people, mostly blue-collar workers, who were faithful available, and teachable. Regular people like them – and like us – can follow the fourfold process of the greatest person ever to live in order to leave a lasting legacy for God’s glory. (Ingram, 2017, p. 254)

Ultimately growing and extending God’s kingdom in a Christ-like manner is the end goal of a Christian educator. During the journey of each student, the Christian educator is to be a shepherd and watch the students as if they were sheep. Ensuring their overall well-being by keeping watch of them, protecting them from predators, and seeking and finding them when they stray from the protection of the shepherd. These actions of the shepherd take an enormous amount of time with the sheep (students) while ensuring their hearts are kept on Christ. Campbell (2016) describes this relationship.

Walking humbly with God is a lifelong journey, and many of the spiritual exercises, disciplines, and realities of the Christian life do not deliver everything instantly with little or no effort … As (the Christian leader) commits to being with (the student) on the journey, (the Christian leader) can help them recognize when their desire for instant gratification has become an idol drawing their worship away from God.” (p. 140)

A Christian educator must understand that Christ was intentional with His life. As Ramsey (2011) states,

There was purpose behind everything (Mary’s) son ever did. It was in his words. It was in his ways. It even seemed that he hung on that cross because he meant to. (Mary’s) son wasn’t simply dying. He was doing something. (p. 155)

Educators must be intentional with the Christian values and lessons they are teaching their students. If the educator is not intentional with their actions and lessons, how can the educator state the collegiate experience they are providing the sons and daughters of parents (who may be financially supporting their child’s Christian education) is truly grounded within Christian values and ethics? As Christ was intentional with everything He did here on earth, Christian faculty members must do the same to create an impact that is directed towards Christ.
Knight (2006) describes how the Christian educator is not just in the role to help students know more and become better workers. Knight shares that the Christian educator’s role includes leading the students towards understanding and relating better with Christ to be ready to perform God’s work for His glory and kingdom.

Teaching is much more than the passing on of information and fillings students’ heads with knowledge. It is more than helping them prepare for the world of work. The primary function of the teacher is to relate to the Master Teacher in such a way that he or she becomes God’s agent in the plan of redemption. (Knight, pp. 212-213)

Commitment

As the Christian faculty member must be intentional, one item the Christian educator must be intentional about is being committed to Scripture and the calling of a Christ-follower and Christian leader. Bredfeldt (2006) remarks “This foundational commitment to the authority of Scripture marks the Evangelical. It must also be the distinguishing characteristic of the biblical leader. Biblical leaders are committed to biblical authority and to the absolutes of Scripture” (p. 70). John C. Maxwell describes how Paul could have fallen into temptation by not being as committed as he needed to be to perform God’s work. Maxwell (2007) takes this lesson and relates it to a modern-day Christian leader that has lost the commitment to the church and the Trinity by being tempted by something ungodly.

Paul says in 1 Corinthians 7:24, “Brethren, each one is to remain with God in that condition in which he was called, “Remember when Paul stood before King Agrippa and said, “I did not prove disobedient to the heavenly vision.” Paul could have been tempted to give up, take other options, or yield to the persecution, but the thing that kept him on track was the vision before him. The world continually thrusts opportunities at us that would distract us from God’s call. There is nothing more tragic than when a Christian leader loses God’s anointing on his life by allowing himself to become sidetracked. There is no higher violation of God’s trust. For when a leader stumbles, others fall. (Maxwell, 2007, pp. 113-114)

Murray Harris discusses how being a slave to Christ, as Paul called himself in Romans 1:1 (variations across translations include slave, bondservant, and servant) is the role of a
believer. This idea of being a slave to Christ is as committed of a term as one can think of.

“Believers give satisfaction to their Master not only by obeying him, but also by devising innovative ways of pleasing him. ‘We make it our ambition’, says Paul, ‘to be constantly pleasing to him’ (2 Cor. 5:9)” (Harris, 2001, p. 143). The Christian educator must be focused on serving others, including the students. This servanthood from the leader should be a direct response to the educator being a servant of Christ and striving to be like Christ. If these two underlying themes are true for the teacher, understanding and striving to serve the student should be a product of those beliefs. Pettit (2008) discusses how the ultimate example of humble service is the portrait of Christ as described by select verses in Philippians Chapter 2.

What we do best is God’s gift to us, what we do with that talent is our gift to God. Our ministry is our special place of service in and within the body of Christ. It is a special activity done for God and others that is fueled by the Holy Spirit.” (p. 275)

Philippians 2:3-8 (NIV) describes the commitment to serving others as Christ served.

Do nothing out of selfish ambition or vain conceit. Rather, in humility value others above yourselves, not looking to your own interests but each of you to the interests of the others. In your relationships with one another, have the same mindset as Christ Jesus: Who, being in very nature God, did not consider equality with God something to be used to his own advantage; rather, he made himself nothing by taking the very nature of a servant, being made in human likeness. And being found in appearance as a man, he humbled himself by becoming obedient to death—even death on a cross! (NIV, Phil. 2:3-8),

Character

John Wooden, a devout Christian and arguably the greatest basketball coach of all time, stated at a TED talk in 2001, “Your reputation is what you’re perceived to be; your character is what you really are. I think that character is much more important than what you are perceived to be. You’d hope they’d both be good” (Wooden, 2001). Having a good reputation is also a qualification of a Christian leader as stated in 1 Timothy 3. Bredfeldt describes the differences between character versus other traits such as values and servanthood and how character is more
than both values and servanthood while describing the differences between values and virtues.

Bredfeldt (2006) states,

Values are crucial and servanthood is certainly the summary term for biblical leadership, but character is more than values or servanthood. From a biblical perspective, character is the consistent enactment of biblical values through the power of Christlike virtues.” (p. 89)

Below are different characteristics of values and virtues that make them different, according to Bredfeldt (pp. 89-90).

Values:
- Principles, standards, or qualities considered worthwhile and desirable
- Beliefs that a person or group holds
- Have an emotional investment and heartfelt commitment

Virtues:
- Moral excellencies
- Qualities of righteousness corresponding to the nature and character of God
- Universally morally correct, due to being drawn from God
- Internal and part of our moral fabric producing the longing to always do what is right

Besides the commitment to be like Jesus, another Scripture reference that can be utilized to create the foundations of characteristics of a Christian educator, due to being a Christian leader of a pastoral role, can be found in 1 Timothy 3.

Here is a trustworthy saying: Whoever aspires to be an overseer desires a noble task. Now the overseer is to be above reproach, faithful to his wife, temperate, self-controlled, respectable, hospitable, able to teach, not given to drunkenness, not violent but gentle, not quarrelsome, not a lover of money. He must manage his own family well and see that his children obey him, and he must do so in a manner worthy of full respect. (If anyone does not know how to manage his own family, how can he take care of God’s church?) He must not be a recent convert, or he may become conceited and fall under the same judgment as the devil. He must also have a good reputation with outsiders, so that he will not fall into disgrace and into the devil’s trap. In the same way, deacons are to be worthy of respect, sincere, not indulging in much wine, and not pursuing dishonest gain. They must keep hold of the deep truths of the faith with a clear conscience. They must first be tested; and then if there is nothing against them, let them serve as deacons. (NIV, 1 Timothy 3:1-10)
Chester and Timmis (2008) share how character is more important than the educational background of the Christian teacher. Chester and Timmis utilize Paul’s work as proof that character is a more desirable trait than skills.

“Paul had the highest education possible (Acts 22:3). It is not bad to be highly educated. But the qualities he outlines for Christian leaders are not skills-based but character-based. The focus in 1 Timothy 3 and Titus 1 is on the character of leaders – their godliness, their maturity, their example. The only skill needed is the ability to teach – and that does not necessarily mean giving forty-five-minute sermons. It is the ability to apply God’s word to the life of the church and the lives of its members.” (p. 120)

**Qualifications**

As stated in the previous section, 1 Timothy 3 highlights the qualifications of a Christian leader. Knight (2006) lists various qualifications for a Christian teacher that accurately encompasses this theological framework of the role of a Christian faculty member.

There are spiritual, mental, social, and physical characteristics that are important qualifications for Christian teachers … they have a personal saving relationship with Jesus … be students who are continually growing in their own mental development … teacher can offer their students the gift of companionship in work and play. It is important to build relationships outside the classroom if teachers are to be successful inside of it … Christian teachers should, therefore, be individuals who seek physical health and balance in their own lives through following the laws of health that God has built into the natural world and reveals in His Word. (pp. 219-220)

The one, and final, aspect that has not been addressed in this theological framework that Knight describes is the qualification of offering the gift of companionship in work and play to build the relationship between the teacher and student outside of the classroom. This idea of being a companion to students outside of the classroom may appear radical, irresponsible, or dangerous to Christian educators; however, did not Christ spend time with His disciples and believers outside of His teachings? Is not the student going to be just like the teacher as described in Luke 6? How will the student know how to be like the teacher outside of the classroom if the student is unable to experience and observe the teacher in the real world outside of the classroom?

Spending precious time outside of the classroom and class timeslots is critical for the student to
truly become fully trained and like the teacher. After all, is not Christ always available to us as we are His students? Smith (2011) describes how the places across the ecosystem of the Christian collegiate experience that may have a more formative effect on a student is not within the classroom, but outside of it.

Scholars tend to focus on the “academic” spaces of the university, any discussion of the university as a place of liturgical formation will also tend to focus on those academic sites. But the university’s formative, liturgical power extends well beyond the classroom and the lecture hall. Indeed, it might be that the dorms, stadium, and frat houses are even more powerful liturgical sites within the university – shaping students into certain kinds of people, who develop certain loves, bent on certain ends. (pp. 114-115)

Christian faculty members must spend time with the students inside of the classroom and outside of the classroom if the faculty member wants to offer the gift of companionship to build the relationship as Christ built His relationship with the future leaders of the church.

**Theoretical Framework for the Study**

**Cybersecurity Workforce Shortage**

The cybersecurity workforce shortage continues to be an issue for companies across the globe that have an Internet presence. Without enough skilled talent readily available, companies are left even more vulnerable to cyber-attacks. (ISC)² has been sponsoring and performing cybersecurity/information security workforce research regularly since 2004 ((ISC)², n.d.). The documentation of (ISC)²’s research showing there is a cybersecurity workforce gap can be seen as early as *The 2013 (ISC)² Global Information Security Workforce Study* where 56% of respondents believed a cybersecurity workforce shortage was present (p. 4) and (ISC)² stated “the impact of [the cybersecurity] shortage is the greatest on the existing workforce” (p. 4). The *2019 Cybersecurity Workforce Study* elaborated on the cybersecurity workforce gap by estimating the number of cybersecurity professionals needed to fill gaps in the global economy.

In the U.S., the cybersecurity workforce gap is nearly 500,000. By combining our U.S. cybersecurity workforce estimates and this gap data, we can calculate that the
cybersecurity workforce needs to grow by 62% in order to meet the demands of U.S. businesses today. Using the workforce estimate of 2.8 million based on the 11 economies for which we provided a workforce estimate and the global gap estimate of 4.07 million, we can estimate that the global workforce needs to grow by 145%. ((ISC)², 2019, p. 8)

Companies without adequate cybersecurity personnel and resources may not even know they are being attacked. Mandiant, owned by FireEye, found the global median dwell time (the time it takes for an attacker to be discovered on a network) was lowered to 24 days. This is a shocking number as some other statistics show that this number might be closer to 207 days to identify a breach (IBM, 2020, p. 11). It should be noted that the types of attacks can significantly alter the time it takes to discover a cyber-attack (e.g., a ransomware that locks out all computers and demands money be sent to the attackers would have a dwell time of 0 days due to it being obviously discovered).

Companies that are unable to fill their need for enough qualified and skilled cybersecurity professionals are left with finding other ways to manage or temporarily fulfill these tasks that cybersecurity professionals should be handling. Oltsik (2019) suggests most organizations are impacted by the cybersecurity workforce shortage.

For the third year in a row, the ESG/ISSA data suggest that most organizations are experiencing the impact of the cybersecurity skills shortage in one way or another. Cybersecurity professionals (and especially CISOs) must assume that they will be short on people and skills in every decision they make and every project they undertake. (p. 43)

Cybersecurity teams that either do not have enough skills, enough people, or both are left with finding other ways to lower the risks their company faces in the cyber domain. Oltsik also describes some of the ways companies can lower the cyber risk without increasing cybersecurity skills or personnel.

To address the cybersecurity skill shortage directly, infosec pros will need to increase their dependence on managed/professional services, automate manual processes, do everything they can to decrease the attack surface, improve cyber-risk management data analysis, prioritization, and mitigation, and experiment with more use of advanced analytics technologies. (p. 43)
The National Nuclear Security Administration (NNSA) is currently looking for roughly 2,000 nuclear security professionals (including cybersecurity professionals) across ten different locations across the United States (Hamilton, 2021). If the NNSA is unable to obtain enough qualified and talented cybersecurity professionals, the nuclear operations are at a greater risk of exposure!

Government Involvement

The United States government has had a vested interest in developing cybersecurity professionals for years. This is seen by the NSA/CAE program, the CyberCorps Scholarship for Service, FedVTE, and other programs developed, funded, or supported directly or indirectly by the government. The NSA has established an NSA/CAE accreditation process that promotes academic institutes that meet a rigorous list of objectives. The three possible designations an institution can receive are the: Cyber Defense Education (CAE-CDE) designation; Cyber Research (CAE-R) designation; and Cyber Operations (CAE-CO) designation. The National Centers of Academic Excellence (CAE) is a program sponsored by DHS and NSA where institutions of higher education can be designated as a CAE if their degree programs meet strict requirements that include an alignment between critical cybersecurity skills and Knowledge Units (KUs). There are over 200 educational institutions that have earned the distinction as either a CAE in Cyber Defense Education (CAE-CDE), or CAE in Cyber Operations (CAE-CO) (CISA, 2019). CISA provides an overview of the differences between these three designations; CAE-CDE, CAE-CO, and CAE-R.

The CAE-CDE designation is awarded to regionally accredited academic institutions offering cybersecurity degrees and/or certificates at the Associates, Bachelors and graduate levels. The CAE-R designation is awarded to DoD schools, PhD producing military academies, or regionally accredited, degree granting four-year institutions rated by the Carnegie Foundation Basic Classification system as either a Doctoral University - Highest Research Activity (R1), Doctoral University - Higher Research Activity (R2), or
Doctoral University - Moderate Research Activity (R3). The CAE-CO designation is a deeply technical, inter-disciplinary, higher education program firmly grounded in the computer science, computer engineering, and/or electrical engineering disciplines, with extensive opportunities for hands-on applications via labs and exercises.” (2019)

The government initiatives have varied widely by either funding scholarship opportunities, such as SFS, funding the development of cybersecurity curriculum for federal government employees and veterans, such as FedVTE, or creating/funding the development of an annual President’s Cup Cybersecurity Competition that has occurred annually since 2019. These examples only describe a few of the government’s positive impacts on increasing the opportunities for cybersecurity professionals to get the skills and education needed.

The federal effort in cybersecurity education, training, and workforce development has not been comprehensively inventoried. However, federal funding supports a wide variety of activities in this area. These activities, which are sometimes offered in partnership with multiple federal and non-federal entities, include cybersecurity awareness (StaySafeOnline.org), summer camps (GenCyber) and student competitions (CyberPatriot and the National Collegiate Cyber Defense Competition), scholarships for cybersecurity postsecondary students who agree to serve in government after graduation (CyberCorps), and professional development for federal personnel in specialized cybersecurity positions (College of Cyber and the Federal Virtual Training Environment). (Jaikaran, 2018, p. 11)

As Jaikaran mentioned, one of the ways the federal government has funded and supported training and hiring cybersecurity talent is through the CyberCorps Scholarship for Service (SFS).

CyberCorps Scholarship for Service, commonly referred to as SFS, covers the tuition expenses of earning a degree in a cyber-related field. This program is sponsored by NSF, and in exchange for the tuition benefit, the graduate is required to work in a government organization for a term equal to the length of their scholarship. As of January 2018, there are 70 participating educational institutions, and over 2,500 SFS graduates have acquired positions in over 140 federal, state, local, or tribal agencies. The program also provides guidance to hiring managers in government agencies on recruiting an SFS graduate. (CISA, 2019)

NSF 21-580 describes in greater detail the vast amount of compensation the SFS Scholarship provides the student during their academic journey while pursuing their associate, bachelor, master, or doctoral degree.
The SFS Scholarship award supports up to three years of stipends, tuition, and allowances for students in the general area of cybersecurity. The scholarships provide academic year stipends of $25,000 per year for undergraduate students and $34,000 per year for graduate students. In addition, SFS scholarships cover expenses normally incurred by full-time students in the institution, including tuition and education related fees (does not include items such as meal plans, housing, or parking); and a professional allowance of $6,000 per academic year for SFS Job Fair and other travel, conferences, research materials and supplies, a laptop, books, professional training and certifications, etc. (NSF, 2021)

**Ethical Behavior**

The importance of ethical behavior is an area that is widely accepted as a crucial pillar of a cybersecurity professional. To highlight this, the following references from popular cybersecurity companies, certification providers, and institutions are below:

**(ISC)² Code of Ethics Canons:**

- Protect society, the common good, necessary public trust and confidence, and the infrastructure
- Act honorably, honestly, justly, responsibly, and legally
- Provide diligent and competent service to principals
- Advance and protect the profession

**Offensive Security’s Core Values:**

- Treat each other as family
- Be passionate in your contribution
- Act with Integrity
- Foster and grow with communities
- Innovate to lead the market

**FireEye**

- Honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships
- Full, fair, accurate, timely and understandable disclosure in reports and documents we file with regulatory agencies and in our other public communications
- Compliance with applicable laws, rules and regulations
- The prompt internal reporting of violations of this Code
- Accountability for adherence to this Code
The companies listed above understand their cybersecurity certifications or services have a great reputation amongst the cybersecurity community, management, and human resources. These codes of ethics serve to ensure professionals that represent their organization (whether by attaining their certification or being an employee) do not tarnish the reputation of others that maintain the same certification or work for the same company while also ensuring the cybersecurity community is improving. If the people charged with cybersecurity are not 100% on board from an ethical perspective, the foundation is already corrupted for positive cybersecurity change to occur.

**Ethics in Cyberspace**

What cybersecurity professionals can organizations trust and why does the color of one’s hat matter? The terms black hat, white hat, and gray hat metaphorically speak to the ethical intentions of a cybersecurity ‘person’. This researcher refrains from calling somebody who is not ethical a cybersecurity ‘professional’. It should also be noted that this researcher supports altering the terms black hat, white hat, and gray hat to avoid using controversial color naming techniques (even though the roots may be tied to old western movies); however, the cybersecurity lexicon has not seen this shift, yet (Cimpanu, 2020). Regardless, from a high-level viewpoint; a white hat is one with clear ethical boundaries and required permissions to attack a system; a black hat is one with no ethical boundaries and does not have permission to attack a system; a gray hat is in the middle between the two due to ethical decisions, permissions, or intent. In addressing this issue, Aidan Knowles, an Ethical Hacking Engineer for IBM, defines what he calls the "rainbow of hackers". He groups hackers into three categories—black hats (the bad guys), white hats (the good guys), and gray hats (somewhere in between). As Knowles states, the three types of hackers carry out similar actions. They all use the same tools and
resources to target various aspects of computer infrastructure—applications, networks, systems, hardware, and software as well as people. What differentiates their activities are motivation, legality, permission, and pre-knowledge of others regarding their actions. Each type of hacker has a different goal in mind for their work and different characteristics, as Knowles indicates:

White hat:

- Commonly employed or contracted to carry out an attack
- Have explicit permission and clear-cut boundaries from the organization
- Research, find, and test vulnerabilities, exploits, and viruses in their defined targets
- The findings of these professional engagements are reported directly to the target to enable them to fix any holes and strengthen their overall security posture
- Sometimes involved in developing security products and tools

Black hat:

- Cause great intentional damage and profit at the expense of their targets
- Can include cybercriminals, cyber spies, cyber terrorists, and hacktivists
- Can be an external threat actor or an insider threat
- May develop their own malicious tools but will frequently employ or repurpose existing white-hat software

Gray hat:

- Their work may be classified as leaning toward good or bad on the spectrum depending on your perspective
- The term gray hat is sometimes used to describe those who break the law but without criminal intent
- May include cyber vandals who deface websites and so-called rogue security researchers who publicly share discovered vulnerabilities without notifying or receiving prior permission from their targets (Knowles, 2016)
"Without clear ethical standards and rules, cybersecurity professionals are almost indistinguishable from the black-hat criminals against whom they seek to protect systems and data." (Knowles, 2016)

Over 4.7 billion people throughout the world utilize the Internet, as of April 2021 (DataReportal, 2021). The integration between the Internet and the real-world life of an Internet user continues to be more intertwined. The typical global Internet user now spends 3 hours and 39 minutes each day using the Internet from a mobile phone and 6 hours and 54 minutes each day using the Internet from all devices (2021). The utilization of the Internet by Internet users to perform daily life and even significant life events continues to rise. Utilizing the Internet to purchase houses without visiting the property via recorded or live walkthrough virtual tours of houses or use of 3D virtual tours with 3D technology, such as Matterport, has become a reality. Utilizing Internet sites to research vehicle reviews and comparing vehicle prices from different dealerships is nothing new; however, Internet users can utilize websites, such as Carvana, to purchase vehicles and have the vehicle delivered to you without you having to leave your home. With the rise of Internet utilization, purposes, and users, the role of a cybersecurity professional continues to rise in importance to global society’s security and privacy. The role of a cybersecurity professional can vary greatly; however, the ethics behind how the cybersecurity professional conducts themselves should remain steadfast.

The NICE Framework, NIST Special Publication 800-181 Revision 1, has deprecated categories of cybersecurity professionals; however, state “organizations that find value in the former Categories … can continue to use them”. These categories are Analyze, Collect and Operate, Investigate, Operate and Maintain, Oversee and Govern, Protect and Defense, and Security Provision. Each of these categories of cybersecurity jobs requires an ethical approach to
deliver a secure, but private, digital world that has real-world implications. Typically, there is a conflict between security and privacy; however, fairness and accountability must also be considered when a cybersecurity professional deals with ethical dilemmas (van de Poel, 2020). Christen et al. in their work *A Review of Value-Conflict in Cybersecurity: An assessment based on quantitative and qualitative literature analysis*, describe the ever-growing importance of cyberspace and the digital ecosystem alongside increased global risks has created a dilemma. “Overemphasizing cybersecurity may violate fundamental values like equality, fairness, freedom, or privacy. On the other hand, neglecting cybersecurity could undermine citizens’ trust and confidence in the digital infrastructure as well as in policy makers and state authorities” (Cristen et al., 2017, pp. 1-2). In Figure 1, Cristen et al. (2017) showcase the ethical decisions and role of a cybersecurity professional mapped out to show the context of the supporting relations (bolded lines) and conflicting relations (dotted lines).

**Figure 1**

*Christen et al.'s First Draft of a Map on Value Conflicts in Cybersecurity*

Cybersecurity professionals are to protect and defend their customers’ data and devices. Google reports that as of April 17, 2021, 90% of webpages that were loaded in their Chrome
browser by Internet users on a Windows operating system were using HTTPS (encrypted network traffic) (Google, 2021). Cryptographically secure encryption is a popular implementation for a cybersecurity professional when they know what the data is and are trying to prevent unauthorized access to the data; however, encryption that is on a network that cybersecurity defenders do not know can make detecting threats and responding to incidents difficult to perform. Do cybersecurity professionals utilize technologies, like PolarProxy, to create a transparent TLS proxy that intercepts and decrypts TLS traffic for the cybersecurity professional to analyze in a non-encrypted format (cleartext/HTTP) while leaving the encrypted traffic (HTTPS) on the network/Internet? This assists with the ability to detect malware and incidents; however, everything that the user believed was encrypted (usernames, passwords, websites, searches, etc.) is still encrypted to everybody, except the cybersecurity professional that has access to the network traffic that was captured by PolarProxy. Cybersecurity professionals can use tools such as Arkime, Wireshark, or NetworkMiner to analyze this network traffic that is most likely all in cleartext now. Does this increase the cybersecurity of the company? Does it invade the privacy of the customers and/or employees being monitored? Do the customers/employees know they are being monitored? These are a few of the ethical dilemmas that cybersecurity professionals and teams face on a daily basis. Hjelmvik (2020a) showcases in Figure 2 how PolarProxy can be logically implemented to decrypt network traffic for analysis while ensuring the data remains encrypted over the Internet. Hjelmvik (2020b) showcases in Figure 3 how decrypted network traffic can easily reveal messages, images, files, credentials, and more.
Figure 2

*Process of Decrypting Encrypted HTTPS Traffic to Cleartext HTTP Traffic*

![Diagram showing the process of decrypting encrypted HTTPS traffic to cleartext HTTP traffic.]

Figure 3

*NetworkMiner Example of Decrypted HTTPS Traffic*

![Screenshot of NetworkMiner interface showing decrypted HTTPS traffic.]
Cybersecurity Certifications

The number of cybersecurity certifications that are present is arguably overwhelming to entry-level cybersecurity professionals. There has been such a demand for cybersecurity certifications that companies such as (ISC)², SANS, CompTIA, EC-Council, and others have had the opportunity to create their own certifications to help continue to build their brand while helping cybersecurity professionals gain credentials for different areas of cybersecurity. CompTIA has created an IT certification roadmap that helps cybersecurity professionals navigate through the seemingly endless certification opportunities out there based on a job role.

Figure 4
CompTIA's IT Certification Roadmap

Knapp et al. describe several of the popular cybersecurity certifications and their differences that are included along with the plethora of cybersecurity certifications found in the roadmap above.

Removed for copyright.

This figure can be found on CompTIA’s website at https://partners.comptia.org/docs/default-source/resources/08314-it-certification-roadmap-nov2020-update-8-5x11-online
Different certifications will have different foci. For example, many certification exams stress broad knowledge and concepts such as the CISSP. Other certifications focus on specific technologies or infrastructure (e.g., Certified Cloud Security Professional). Some certifications focus on tools and techniques, like the Certified Ethical Hacker (CEH) credential. The Global Assurance Certification (GIAC) offers dozens of specialized certifications aimed to ensure an individual has the skills necessary as a practitioner (GIAC, 2016). Advanced certifications like the Licensed Penetration Tester (LPT) and Offensive Security Certified Professional (OSCP) require a hands-on penetration test demonstration in a cyber-range. (Knapp et al., 2017, p. 106)

**Cybersecurity Curriculum**

Creating a cybersecurity curriculum that is relevant to the workforce, utilizing current versions of technologies, and that faculty members have years of experience working with is a difficult, if not impossible tasks, for programs and institutions. One reason is due to the rapid speed that technology and related vulnerabilities sweep the industry. For example, the software technology Kubernetes was released in June 2014 and was widely adopted across the software and application industry as it allows for automating deployment, scaling, and managing containerized applications (Kubernetes, 2021). In late 2017, the CVE-2017-1002101 vulnerability was discovered and affected a wide array of Kubernetes versions that allowed the containers to access files/directories outside of the container (including the host) (NIST, 2019). This vulnerability, using CVSS Version 3.x has been given a High and Critical base score by different analysts (2019). Considering that this technology was released, adopted widely by industry, and created such vulnerabilities to systems in under four years highlights the rapid speed that cybersecurity faculty members face while staying current with technology and trends while also developing and updating curriculum. A cybersecurity student that is enrolled in a four-year cybersecurity undergraduate program would need to be prepared to implement and defend technologies such as Kubernetes that did not even exist (publicly) when they initially enrolled in the program! Knapp et al. (2017) elaborate on the importance of modernizing mature and new cybersecurity programs to stay current with the field.
Developing course objectives that are relevant and applicable is of key significance to such a rapid developing field like cybersecurity. Even highly successful programs can quickly fall behind the curve if their curricula is not adequately modernized to reflect the current state of the field. While the current paper strives to provide guidelines to academicians who wish to update and maintain their existing programs, the same approach can also provide value to those looking to create a brand new program. (p. 107)

When a faculty member is tasked with not only creating a current curriculum that is relevant to the needs of the industry, the faculty member must ensure the curriculum is developed in an optimal way that students learn the foundational cybersecurity concepts and the hands-on skills to perform the actual cybersecurity work. The faculty member also faces a difficult scenario of assessing how well the students understand the concepts and perform the work. “Both training and education play a role in developing the necessary cybersecurity knowledge base” (Bicak et al., 2015, p. 100). If the curriculum is built with mostly readings and writing assignments, the students may be prepared to speak and communicate regarding cybersecurity topics but will lack the hands-on capability as their program’s curriculum did not integrate hands-on capabilities. The same is true for curriculums that perform an overwhelming number of hands-on activities and lack the instruction of foundational and theoretical concepts.

Galyardt (2019), in an artificial intelligence engineering blog, addresses how cybersecurity researchers do not have time to research the best methods to educate and train cybersecurity professionals as the workforce needs skilled professionals now in this new industry.

Cybersecurity training has unique qualities that make assessing skills challenging. Assessing the viability of training is not a problem that is unique to the field of cybersecurity, but the dynamism of the field is. Algebra, for example, has not changed much in the past 100 years, and the field of calculus has been relatively stable for the past 60. Cybersecurity, on the other hand, requires that those working in the field regularly and periodically learn and practice new skills. As a result, researchers in cybersecurity don't have 20 years to research optimal ways of teaching people how to do things. (2019)
Cybersecurity faculty members are tasked with finding the correct balance of education and training throughout their cybersecurity curriculum.

Education can be considered strategic and provides the foundation for the context for security concepts, tools, technologies, etc., and is acquired through formal studies over a period of time. Cybersecurity training may be considered tactical and puts emphasis on explicit skills. (Bicak, 2015, p. 100)

One of the challenges cybersecurity faculty members have is not only what balance of education and training to provide, but how to assess the technical hands-on capabilities of the students. Cybersecurity students may be given a simulated lab environment where they are told exactly what commands to run and options to select. This may give way to a popular method of delivering hands-on cybersecurity exercises; however, this may not be the best approach as the lab is set up to be a perfect utopia with no troubleshooting or real-world issues. Also, this approach may not be best as the students were told the commands and options to enter, so there was no critical analysis of the situations, but just copying the text from the instructions to the lab environment. This is just one of the methods cybersecurity faculty members may use to gauge how well their students can perform the hands-on cybersecurity tasks. Other faculty members may give their students not enough guidance and have them research and “figure it out” before they are ready to do such, thus discouraging the student or overwhelming the faculty member with inquiries from students who are unable to reach this level of cybersecurity tasks yet.

Conklin describes how the industry is looking for students who have both the education and training to be able to work upon hiring and be able to adapt and continue to operate when technology and other environmental circumstances change.

One of the biggest current gaps in alignment between education and industry is a complaint that graduates do not have sufficient hands-on skill sets to make them ready to perform jobs … The central theme of this issue is training versus education. Training tends to be oriented towards the how and is focused on the current technology and methods … Education tends to focus on the why, the theory and mechanisms behind the material … Industry wants workers to arrive ready to work on day one, on their
equipment, configured as they have configured it, and able to immediately add to the

Industry also expects their workers to have the knowledge (read education) that they can adapt to technology changes and continue to contribute as systems, equipment and processes change … It is important that students learn the theory, the why, as well as how to implement it on current equipment, the how. (Conklin, 2014, p. 2010)

**Related Literature**

**Rationale for Study**

This research study explores the current state of Christian four-year cybersecurity programs. The purpose of this literature review is to establish various contributors of relevance towards creating Christian cybersecurity programs. To achieve this, literature on cybersecurity curriculum standards, cybersecurity curriculum practices, Christian education, and other literature that discusses higher education with Christian education or cybersecurity education are reviewed and presented. This literature review’s focus is to establish commonality between cybersecurity programs, standards, frameworks regardless of spirituality while also ensuring this knowledge can be applied in a Christian environment with a biblical perspective. Upon completion of this literature, assessing current Christian programs and identifying strengths and areas of improvement for current cybersecurity degree programs will have the literature backing and support for each area.

**Curriculum Standards**

Currently, there is not a governing body that requires undergraduate cybersecurity programs to meet certain cybersecurity standards. There is also not an exam that a graduate must take to be accepted into the field. This allows cybersecurity programs the flexibility to create courses and content as the program sees fit. This flexibility in such a new and vast field may lead to two cybersecurity students from different institutions receiving a vastly different educational experience while both receiving a four-year degree in the same field, cybersecurity. This section
discusses different voluntary curriculum standards that undergraduate cybersecurity programs may pursue to bolster and add validity to their program.

**NSA/CAE Accreditation**

In their work, *The Role of CAE-CDE in Cybersecurity Education for Workforce Development*, Maurice Dawson (University of Missouri), Ping Wang (Robert Morris University), and Kenneth Williams (American Public University) explain the NSA’s CAE-CDE Program criteria and requirements while also discussing the great importance the program that is sponsored by the NSA and DHS serves cybersecurity programs (Dawson et al., 2018). At the time of the writing, each of the three universities represented was at three different stages of the NSA/CAE accreditation process; The University of Missouri-St. Louis obtained NSA/CAE accreditation, American Public University System had just completed the application, and Robert Morris University was in the process of applying for designation. Utilizing three different faculty members of three different universities at different stages of the NSA/CAE process offers a unique blended and balanced viewpoint of the CAE-CDE program and process. These three faculty members chose to seek out the NSA/CAE accreditation to highlight their ability to teach their students the cybersecurity topics and skills that potential employers need. “Out of over 5300 colleges and universities in the U.S., only about 200 of them have achieved the CAE-CDE designation status. Attendance at a CAE school will give students confidence in learning, and a degree from a CAE school will give employers confidence in hiring” (Dawson et al., 2018, p. 1). The NSA/CAE accreditation program is intended to help community colleges, four-year programs, graduate programs, and doctoral programs with a means to utilize their framework to build their program and gain reputation by reaching this accreditation. Dawson et al. describe the timeline of the development of the NSA/CAE program.
The national CAE-CDE program evolved from the initial national CAE in Information Assurance Education (CAE-IAE) program started by NSA in 1998 with DHS joining as a co-sponsor in 2004, and the CAE in IA Research special designation was added in 2008 to encourage doctoral level research in cybersecurity. In 2010, the CAE2Y component was created to provide the CAE designation opportunity for two-year institutions, technical schools, and government training centers. Hence, the current CAE-CD program includes these designations: CAE2Y for two-year institutions, and CAE-CDE for four-year institutions, and CAE-R for doctoral universities or Department of Defense schools. All regionally accredited two-year, four-year and graduate level institutions in the United States are eligible to apply for the appropriate CAE designation. The designation is granted to schools which have demonstrated compliance with rigorous CAE criteria and curricula mapping to a required core set of cyber defense knowledge units (KUs) with optional Focus Areas. (Dawson et al., 2018, p. 2)

**NICE Cybersecurity Workforce Framework**

In their work, *Cybersecurity Workforce Development Directions*, Ronald C. Dodge (United States Military Academy), Costis Toregas (The George Washington University), and Lance Hoffman (The George Washington University) discuss and define the requirements for developing the cybersecurity workforce.

The NICE Cybersecurity Workforce Framework organizes the cybersecurity workforce into seven high-level categories, each comprised of several specialty areas. In developing the framework, NIST coordinated with all sectors of the US federal and state government(s) as well as a large number of not-for-profit organizations including educational, security practitioners, and professional societies. (Dodge et al., 2012, p. 8)

These high-level categories of the NICE Cybersecurity Workforce Framework are:

- **Analyze**: Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

- **Collect and Operate**: Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

- **Investigate**: Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

- **Operate and Maintain**: Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

- **Oversee and Govern**: Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
• **Protect and Defend**: Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.

• **Securely Provision**: Conceptualizes, designs, procures, and/or builds security information technology (IT) systems, with responsibility for aspects of system and/or network development. (NIST, 2021)

Dodge et al. (2012) describe how each of these categories are broken down into different specialty areas (SA) with different tasks, competencies, and KSA (knowledge, skills, and abilities).

For example, the “Operate and Maintain” category is further defined to include the following specialty areas: Data Administration, Information System Security Management, Knowledge Management, Customer Service and Technical Support, Network Services, System Administration, and Systems Security Analysis. These seven areas make up the functional requirements within this category. While the breakdown of the categories into specific specialty areas is important, more details are needed to ensure the functions are uniformly understood and supported. To meet this requirement, each specialty area is further defined using the taxonomy shown in [the table below and] are explained in detail for each specialty area so that the job functions within the specialty area are clearly articulated and measurable. (p. 8-9)

**Table 1**

*Taxonomy of Specialty Area*

<table>
<thead>
<tr>
<th>Cybersecurity Category</th>
<th>A generalized grouping of specialty areas</th>
<th>Can have one or more unique specialty areas associated with a category</th>
</tr>
</thead>
</table>
| Specialty Area (SA)    | Defines specific areas of specialty within the cybersecurity domain | • Belongs to one and only one cybersecurity category  
• Can have any number of unique tasks and KSA's associated with it |
| Task                   | Defines high-level activities that codify a specialty area | • Belongs to one and only one cybersecurity specialty area  
• Tasks are not linked individually to competencies/KSA's |
| Competency             | A measurable pattern of knowledge, skills, abilities, or other characteristics that individuals need to succeed and that can be shown to differentiate performance. | • One or more KSA's are assigned to each competency  
• The same competency is likely to be needed across multiple specialty areas |
| KSA                    | Defines a specific knowledge, skill, ability. | • Assigned to one or more specialty areas  
• Each KSA has exactly one competency associated with it |
In their work, *Toward Standards in Undergraduate Cybersecurity Education in 2018*, Rajendra K. Raj (Rochester Institute of Technology) and Allen Parrish (United States Naval Academy) discuss the CSEC 2017 curricular guidelines, as well as the NSA/CAE accreditation and ABET accreditation.

Building on earlier efforts, such as the Cyber Education Project (which was created with the purpose of developing undergraduate curriculum guidelines and a case for formal program accreditation), the CSEC 2017 curricular guidelines are intended to be the leading resource of comprehensive cybersecurity curricular content for global academic institutions seeking to develop a broad range of cybersecurity programs at the post-secondary level. (Raj & Parrish, 2018, p. 73)

Raj and Parrish describe how the CSEC 2017 curricular guidelines are not intended to define a program, but describe the wide array of disciplines (e.g., computer science, computer engineering, etc.) that cybersecurity can be taught within as an interdisciplinary degree. The CSEC 2017 guidelines are utilized for ABET accreditation as discussed in the next section.

Table 2 showcases CSEC 2017 Models of Cybersecurity as described by Raj and Parrish (2018).

**Table 2**

<table>
<thead>
<tr>
<th>CSEC 2017 Model of Cybersecurity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Knowledge Areas</strong></td>
</tr>
<tr>
<td>Data security, software security, component security, connection security, system security, human security, organizational security, societal security</td>
</tr>
<tr>
<td><strong>Crosscutting Concepts</strong></td>
</tr>
<tr>
<td>Confidentiality, integrity, availability, adversarial thinking, systems thinking</td>
</tr>
<tr>
<td><strong>Disciplinary Lenses</strong></td>
</tr>
<tr>
<td>Computer science, computer engineering, information systems, information technology, software engineering, mixed disciplinary</td>
</tr>
</tbody>
</table>
**ABET Cybersecurity Accreditation**

In the same work as described within the CSEC 2017 section, Raj and Parrish (2018) discuss how the ABET accreditation criteria for cybersecurity is a viable option for cybersecurity programs. ABET is a certified organization that accredits college and university programs in applied and natural science, computing, engineering, and engineering technology. Recently they have released guidelines for both cybersecurity accreditation and cybersecurity engineering accreditation (ABET, 2021). In 2018, the first ABET-accredited cybersecurity baccalaureate degrees were at the U.S. Air Force Academy, U.S. Naval Academy, Towson University, and Southeast Missouri State University after the institutions underwent an 18-month process that began in January 2017 (ABET, 2018). The ABET cybersecurity accreditation is guided by CSEC 2017 and was developed by ABET working closely with the Cyber Education Project (CEP), IEEE, and CSAB. A graduate of the ABET CAC cybersecurity accredited program is to have five core outcomes that relate to all aspects of computing and one additional outcome specific to cybersecurity (number six). These six outcomes are:

1. Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.

2. Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program’s discipline.

3. Communicate effectively in a variety of professional contexts.

4. Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.

5. Function effectively as a member or leader of a team engaged in activities appropriate to the program’s discipline.

6. Apply security principles and practices to maintain operations in the presence of risks and threats. (ABET, 2020, pp. 3-8)
Raj & Parrish describe how there was a seventh item regarding analyzing and evaluating systems; however, that is no longer listed as a requirement on ABET documentation. Raj & Parrish argue that if a program is already accredited by NSA/CAE, it will likely be accreditable by ABET as well. Cybersecurity programs have the flexibility to seek NSA/CAE accreditation, ABET accreditation, both, or neither.

**Curriculum Practices**

Cybersecurity curriculum can include both technical and non-technical courses and content. For example, the NSA/CAE requires five technical core Knowledge Units (KUs) (Appendix A) and five non-technical core KUs (Appendix B). This section will discuss technical, non-technical, and certification-based curricula within cybersecurity programs.

**Technical Curriculum**

In the work, *The Role of CAE-CDE in Cybersecurity Education for Workforce Development*, Maurice Dawson shares the technical courses and components of the University of Missouri-St. Louis’s (UMSL) cybersecurity program. The cybersecurity program at UMSL is a multidisciplinary effort between the Department of Mathematics and Computer Science in the College of Arts and Sciences and the Department of Information Systems in the College of Business Administration. Dawson argues this interdisciplinary and collaborative approach increases the collaboration of the various information security and other trends within the industry.

UMSL has created an undergraduate certificate, graduate certificate, undergraduate minor, and graduate track in cyber security. The programs were created to address the shortfall of 3,800+ jobs in the Saint Louis Metropolitan Region. The table below displays the courses for the cybersecurity certificate programs in the Information Systems Department which require students take at least one computer science course. (Dawson et al., 2018, p. 3)
Table 3 (Dawson et al) showcases the different courses required for the cybersecurity certificate at UMSL.

Table 3

*Courses for Cybersecurity Certificate at UMSL*

<table>
<thead>
<tr>
<th>Undergraduate Program</th>
<th>Graduate Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFYS 3848 Introduction to Information Security</td>
<td>INFYS 6828 Principles of Information Security</td>
</tr>
<tr>
<td>INFYS 3842 Data Networks and Security</td>
<td>INFYS 6836 Management of Data Networks and Security</td>
</tr>
<tr>
<td>INFYS 3858 Advanced Security and Information Systems</td>
<td>INFYS 6858 Advanced Cybersecurity Concepts</td>
</tr>
<tr>
<td>INFYS 3868 Secure Software Development</td>
<td>INFYS 6868 Software Assurance</td>
</tr>
<tr>
<td>INFYS 3878 Information Security Risk Management and Business Continuity</td>
<td>INFYS 6878 Management of Information Security</td>
</tr>
<tr>
<td>CMP SCI 4700 Computer Forensics</td>
<td>CMP SCI 4700 Computer Forensics</td>
</tr>
</tbody>
</table>

Dawson et al. share how UMSL offers hands-on components that ensure and enable their students gain a deeper technical educational experience while working with different programming languages, forensics tools, static code analyzers, and offensive security applications to enable the future needs of global cybersecurity.

The UMSL program heavily uses Open Source Software (OSS) as it serves as a means for students to understand low-level coding and to inspect source code for security. Additionally, the labs become reusable learning objects. To enhance student learning, a physical and virtual lab environment was created with both Linux and Windows systems in which the student is given a dedicated Kali Linux virtual machine that allows them to practice offensive security operations in a controlled environment. The lab activities allow students to obtain hands-on experience in offensive and defensive security. (Dawson et al., 2018, p. 3)
As Dawson et al. share regarding the UMSL’s cybersecurity experience, a trend is shown that cybersecurity programs are attempting to give cybersecurity students technical educational experience regarding offensive and defensive cybersecurity abilities. As Conklin stated before, businesses are looking for graduates that can do the technical work on day one. It would appear that UMSL graduates should be ready to work on day one based on Dawson’s description of the program and the NSA/CAE accreditation they possess.

**Non-Technical Curriculum**

Hwee-Joo Kam and Pairin Katerattanakul’s work *Diversifying Cybersecurity Education: A Non-Technical Approach to Technical Studies* describes that cybersecurity is multidisciplinary and in such requires a non-technical approach to curriculum development. They argue that cybersecurity is not limited to the technical aspects of cyber-attacks (e.g., defacing websites), but cybersecurity students must be made aware of the cyber-attacks being influenced by political agenda, and social science and political studies should be infused into cybersecurity education. Kam & Katerattanakul (2014) describe “how cybersecurity education is multidisciplinary that relies on infrastructure, policies, and people and the cybersecurity discipline encompasses psychology, sociology, politics, law, computer science, computer engineering, and management” (p. 1). Their findings regarding integrating non-technical education within technical education confirmed that “processing scientific knowledge occurs in a context-free condition but processing cultural and social elements occurs in a specific social and cultural context and it is difficult to form a bridge between the two” (p. 3). The authors utilized different assignments that required conducting intelligence analysis where the students needed to identify their cognitive and cultural biases when evaluating an event and evaluate different hypotheses for a cyber-attack that was started by a foreign country. The researchers describe two findings regarding how
students may have unknowingly been influenced by the tragic events of September 11, 2001, when attributing a hypothetical cyber-attack against a US banking system and that students did not link their technical knowledge in their reasoning when conducting hypotheses. The authors describe how additional work and research regarding investigating human cognition in terms of making a connection between technical and socio-cultural learning should occur.

Certification-based Curriculum

Dr. Kenneth Knapp, Director of Cybersecurity Programs at Anderson University (SC), previously served as the Director of Cybersecurity Programs at the University of Tampa, published *Maintaining a cybersecurity curriculum: professional certifications as valuable guidance* that discusses the benefits of including certification-driven courses within a cybersecurity program. Knapp et al. argue that utilizing certifications to drive curriculum development as it has been performed with other areas of study, such as accounting, is a valid approach. Knapp et al. discuss the demand for cybersecurity professionals that possess a professional cybersecurity certification by highlighting that “35% of cybersecurity job postings requested a professional certification” (Knapp et al., 2017, p. 102). The author also realizes the plethora amount of cybersecurity certifications that are available to students and professionals and that he does not recommend any one specific certification, but instead urges faculty members to research certifications that can be used to drive and develop educational content for the students.

Knapp et al. reference and agrees with Locasto et al. regarding ensuring that any professional certifications that are utilized should not focus too much on past technologies that are not relevant in today’s industry.

Indeed, there is no reason why faculty should focus on certifications without also covering the latest changes that may not have made their way into certification content.
yet. By taking a strategic approach to selecting a few key certifications to integrate into a curriculum, there should be plenty of room left to incorporate new technologies. (Knapp et al., 2017, p. 106)

Knapp et al. discuss how the faculty at an institution deemed it important to expose students to emerging issues related to critical infrastructure, cyber-physical systems, and the Internet of Things (IoT) while ensuring that no coverage of certification exam material was lost. Knapp et al. also argue that certification bodies are more likely to be enticed to update their content at a faster pace than typical IHLs due to their need for maintaining their reputation and staying relevant. Knapp et al., in Table 4, highlight the percentage of certification material that is integrated into their undergraduate courses.

(ISC)² has refreshed the CISSP exam material approximately every three years since 2009. Therefore, we recommend faculty should find ways to cover material that includes emerging technology and tools while also promoting certifications so students can develop a rounded and relevant education as they enter the workforce. (Kaspersky and Furnell, 2014, pp. 130-133; Knapp et al., 2017, p. 106)

Table 4

**Integrating Certification Material into Undergraduate Courses Matrix**

<table>
<thead>
<tr>
<th>Certification</th>
<th>(ISC)²</th>
<th>ISACA</th>
<th>CISA</th>
<th>EC-Council</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undergraduate Course</td>
<td>CISSP</td>
<td>CISM</td>
<td>CISA</td>
<td>CEH</td>
</tr>
<tr>
<td>Management Information Systems</td>
<td>5%</td>
<td>5%</td>
<td>20%</td>
<td>5%</td>
</tr>
<tr>
<td>Application Development</td>
<td>5%</td>
<td>5%</td>
<td>5%</td>
<td>5%</td>
</tr>
<tr>
<td>Information Security Principles</td>
<td>100%</td>
<td>70%</td>
<td>50%</td>
<td>50%</td>
</tr>
<tr>
<td>Network &amp; Cloud Infrastructure</td>
<td>50%</td>
<td>10%</td>
<td>60%</td>
<td>65%</td>
</tr>
<tr>
<td>Info Security Standards, Risk Mgmt, &amp; Compliance</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>15%</td>
</tr>
<tr>
<td>Network Security</td>
<td>100%</td>
<td>15%</td>
<td>40%</td>
<td>65%</td>
</tr>
<tr>
<td>Ethical Hacking</td>
<td>35%</td>
<td>10%</td>
<td>20%</td>
<td>100%</td>
</tr>
<tr>
<td>Physical and Operational Security</td>
<td>75%</td>
<td>10%</td>
<td>60%</td>
<td>30%</td>
</tr>
<tr>
<td>Cybersecurity Capstone</td>
<td>100%</td>
<td>40%</td>
<td>60%</td>
<td>30%</td>
</tr>
<tr>
<td>Total Coverage of Exam Objectives</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>
**Capture The Flag (CTF)**

A cybersecurity CTF is a competition between cybersecurity professionals and/or students while learning cybersecurity (Harmon, 2016). These CTFs differ in styles from Jeopardy-style, attack-defend (red/blue), king of the hill, linear, and other types (including mixed) (Raymond, 2019; CTF.zone, n.d.). The most popular CTF format is Jeopardy (CTFtime, 2021). In Jeopardy format, participants can select a specific challenge, commonly in a specific category, for a certain number of points relative to the expected difficulty of the challenge. Once a challenge has been solved, typically by submitting some text (usually called a string) that represents a “flag” (e.g., `{TeamEffort}` or `{wh47423y0u90nn4d0?}`) found in the challenge, the challenge on the board has some clear indication that the challenge has been solved (commonly by changing color). Figure 5 is an example of this researcher’s personal CTF website that is utilizing the CTFd platform.

**Figure 5**

*Jeopardy-style CTF Example with 1 Solved Challenge*
These different categories are flexible, depending on the theme of the CTF; however, some common domains are network analysis, web exploitation, forensics analysis, reverse engineering, cryptography, and reconnaissance (MetaCTF, 2020; Gonzalez et al., 2019). These CTFs can also be performed individually, or as a team (National Cyber League, 2021). Hugo Gonzalez, Rafael Llamas, and Omar Montaño utilized an extra class CTF tournament to reinforce knowledge and skills learned during a cybersecurity course that the students were able to vote on the topics before the competition. The results from their research found three pieces of data:

1. The students felt that they are contributing to decide their path on the learning process. They would like to have more courses with a flexible curriculum where they can propose new and interesting topics

2. The students reported that they were more engaged and motivated in the class, most of them felt that their expectations about the course contents were fulfilled in the class.

3. Majority of the students felt well working on the practices. Only two students expressed they were not comfortable with the practices because they found them very technical and found themselves lacking skills to complete the exercises. (Gonzalez et al., 2019)

Gonzalez et al. reflect on the enjoyment and positive experience the faculty encountered while creating the custom, fun, hands-on competition to help the students have yet another encounter with the material that was covered in class.

Designing and developing the challenges was a fun exercise for the instructors and playing them was a great activity for the students to reinforce their skills. The results from the tournament showed that students were learning new skills that they can apply in real-world scenarios. Gamification in the classroom through CTF tournaments should be implemented and practiced in cybersecurity-related courses. (Gonzalez et al., 2019)

Newer cybersecurity programs can utilize publicly available CTFs to help students reinforce concepts learned within cybersecurity, but also expose students to additional topics that have not (or will not) be covered within their specific cybersecurity program. Utilizing this approach helps alleviate the technical stress of relying entirely on developing a new curriculum
from scratch while offsetting the technical burden of hosting and managing a cybersecurity range (whether partially or entirely). Some publicly available CTFs that students can compete in are National Cyber League, iCTF, DC3 Forensic Challenge, CyberPatriot, CCDC, PlaidCTF, CSAW CTF, MetaCTF, and others (National Cyber League, 2021; Gonzalez et al., 2019; MetaCTF, 2021). For example, Anderson University (SC) launched their Center for Cybersecurity in 2019 and their first courses took place in Fall 2020 (Anderson University, SC, 2019). Within this first year, cybersecurity students were not only competing in CTFs, but placed relatively high for a first-year program. “The MetaCTF competition included more than 1,000 teams from around the world. AU's first-year cybersecurity students placed 74th”. This same team, root@au, (coached by this researcher) placed 141st out of 922 teams across the nation during the National Cyber League (NCL) Spring 2021 Competition (Anderson University, SC, 2021a) and 157th out of 920 teams in Fall 2021 (Anderson University, SC, 2021b).

Challenges with Cybersecurity Pedagogy

April Galyardt, a machine learning research scientist, in her blog *Improving Assessments for Cybersecurity Training*, (as mentioned earlier), discusses the challenges cybersecurity education faces with assessing the training for the students. As stated earlier, the global economy is in dire need of cybersecurity professionals as there is a current shortage. Galyardt describes due to this demand and urgent need, researchers do not have the luxury of decades to work on studying optimal methods to teach and train cybersecurity professionals.

Researchers in cybersecurity don't have 20 years to research optimal ways of teaching people how to do things … We cannot directly measure knowledge inside a trainee's head. Instead, we must infer what knowledge they possess, based on things that we can observe. (Galyardt, 2019)

Galyardt continues describing an effective and current method to training and assessing the performance of cybersecurity students. Galyardt (2019) argues that three requirements must be
met to accurately reach a conclusion regarding the effectiveness of the cybersecurity training and the readiness of the student:

1. A domain model. A domain model is the critical mapping between what we can observe (e.g., what commands the trainee entered) and what we want to infer (e.g., that they can secure a network in the future). The domain model is a prerequisite to inform what relevant data looks like. Without an explicit and accurate domain model for cybersecurity task performance, we risk drawing inaccurate conclusions, possibly leading to inaccurate assessments of mission readiness.

2. Relevant data. We cannot distinguish between expert and novice performance if we do not record data on the ways in which they differ. Both novices and experts might be able to complete a task, but the experts are generally faster and use more efficient strategies. If we record only right/wrong, we cannot distinguish performance. If we can record solution time and other features of performance, however, we can then start to model what expert performance looks like.

3. Statistical modeling to compare performance data to expert patterns. Everyone will occasionally "slip" and not give a correct response, even when they know the answer to a problem. (Have you ever made a typo?) To account for these kinds of errors, it is important to probabilistically compare actual performance to expected performance patterns. A good statistical model will explicitly capture the idea that an expert should be more likely than a novice to arrive at a quality solution.

**Identified Gap in the Literature**

As this research attempted to gain a better understanding of undergraduate cybersecurity education, this researcher was unable to identify cybersecurity material from a Christ-centered perspective. The overall topic of integrating cybersecurity programs into Christian colleges is undocumented. Only three of the 140 institutions that are members of the CCCU and located in the United States offer cybersecurity degrees that are recognized by the NSA/CAE (Montreat College, Regent University, and Oklahoma Christian College). This small size justifies how limited are mature cybersecurity programs from a Christian college. Identifying the current state will help current programs get better and provide a framework for newer programs to follow. This research was intended to set the precedence for both future research regarding the effectiveness of Christian undergraduate cybersecurity programs and additional research
regarding the effectiveness of other cybersecurity programs (public, secular private, other religious institutions, distance learning, graduate, etc.).

**Profile of the Current Study**

This study utilized the theological and theoretical frameworks as described within this section to build the process of performing qualitative, exploratory, phenomenological research with understanding student perspectives of their Christian cybersecurity undergraduate program experience. These theological and theoretical frameworks will build the foundation for creating the research instruments and surveys needed to assess the graduates regarding their technical, non-technical, and whole-person development and preparation for the workforce.
CHAPTER THREE: RESEARCH METHODOLOGY

This chapter dives into the qualitative, exploratory, phenomenological research used to identify strengths and gaps recent cybersecurity graduates experienced during their Christian undergraduate experience. The first portion describes the research problem, purpose, questions, design, and methodology within the research design synopsis. The second portion describes the settings, participants, researcher role, ethical considerations, data collection methods and instruments, and finally data analysis.

Research Design Synopsis

The Problem

Gaining a better understanding of how well Christian undergraduate cybersecurity pipelines are preparing the students holistically is optimal to create a feedback loop. This will help ensure that programs continue to thrive and are able to meet the demands of the workforce. This research will allow Christian cybersecurity program leaders to self-assess if their programs have any of the strengths or weaknesses, if identified, to allow the program to continue to improve or change any shortcomings. To this researcher’s knowledge, there has not been widespread research performed measuring the satisfaction of recent graduates from Christian cybersecurity programs regarding their holistic academic experience.

The growth of cybersecurity undergraduate programs continues to rise amongst Christian colleges and universities (Anderson University, SC, 2019; Bob Jones University, 2019; North Greenville University, 2020; Pensacola Christian College, 2019). Institutions such as Anderson University (SC), Pensacola Christian College, North Greenville University, and Bob Jones University are some of the Christian institutions of higher education that have recently launched a new undergraduate cybersecurity program. Currently, as the result of a zero percent
unemployment rate, the need for cybersecurity professionals is so extensive that every graduate that seeks a job will likely find one (Schwartz, 2019). This need for businesses to hire cybersecurity professionals can potentially leave higher education institutions vulnerable to not adequately identifying gaps in their holistic development the student experience during their undergraduate timeframe as each student is being hired. This high-demand situation creates a need to assess the effectiveness Christian cybersecurity programs have had amongst recent graduates that are now in the workforce.

**Purpose Statement**

The purpose of this qualitative, exploratory, phenomenological research was to gain an understanding of the perspectives of recent Christian college and university cybersecurity graduates regarding the holistic experience (technical, non-technical, and whole-person) strengths and shortcomings (if any) of their undergraduate academic program as preparation for the workforce. The categories the graduates utilized to describe their holistic undergraduate education are defined as technical, non-technical, and whole-person. The technical category addressed technical cybersecurity topics (e.g., cryptography; networking; network defense; scripting; hacking; etc.). The non-technical category collected data pertinent to their preparation to perform non-technical cybersecurity topics (e.g., cybersecurity planning and management; policy, legal, ethics, and compliance; security risk analysis; cyber threats; etc.). The whole-person category assessed the non-cybersecurity-related skills and traits they developed at their institution (e.g., love; strength; steadfastness; faithfulness; being on guard; etc.). The gap driving this study is the need to learn how current cybersecurity programs have influenced and molded students for the workforce and allow Christian cybersecurity program leaders to utilize this research and optimize the experience their students have at their institution. The theory guiding
this exploratory research is academic outcomes assessment theory in which student opinions are sought to identify the satisfaction relationship their technical, non-technical, and whole-person development in their Christian undergraduate program as preparation for real-world application.

To this researcher’s knowledge, an exact definition of technical cybersecurity skills does not exist, thus the definition of technical cybersecurity skills is based on technical skills required to fulfill the NSA/CAE Knowledge Units (KUs) technical core. The definition for a technical cybersecurity skill is “a cybersecurity function that primarily relies on the professional to be working directly with cybersecurity technology and have technical control over the information via information technology”. Some of these technical areas are: Scripting and Programming, Networking, Network Defense, Cryptography; and Operating Systems Concepts (NSA/CAE, 2020).

The definition for non-technical cybersecurity skill is the inverse of the technical cybersecurity skill definition and aligns with the NSA/CAE Knowledge Units (KUs) non-technical core. The definition for a non-technical cybersecurity skill is “a cybersecurity function that does not rely on the professional to be regularly working with the cybersecurity technology that is actively performing cybersecurity tasks”. Some of these non-technical areas are: Cyber Threats; Policy, Legal, Ethics, and Compliance; Security Program Management; Security Risk Analysis; and Cybersecurity Planning and Management (NSA/CAE, 2020).

A whole-person approach to education nurtures an integrated development of the mind, heart, and ego of the learner, to foster a holistic and equal growth of what the student understands, what they care about, and their daily actions and behaviors (Mustakova-Possardt, 1998). Educating the whole person is a distinctive shift within higher education and may be one of the most significant and valuable outcomes of learning (Long, 2013; McSweeney, 2015). The
definition for the whole-person criteria is based on Mustakova-Possardt, Long, and McSweeney’s research and does not relate to cybersecurity. The definition for whole-person development is “any skill, education, or molding that is not primarily and/or directly related to cybersecurity, but growth as an adult”. The theory that guided this study was to identify the satisfaction relationship between recent cybersecurity graduates and their technical, non-technical, and whole-person development at their Christian undergraduate program. Cybersecurity programs have influenced and molded students for the workforce and allow Christian cybersecurity program leaders to utilize this research and optimize the experience their students have at their institution.

**Research Questions**

**RQ1.** How would a recent graduate describe, if any, technical skill strengths and gaps commonly experienced in Christian cybersecurity undergraduate programs?

**RQ2.** How would a recent graduate describe, if any, non-technical skill strengths and gaps commonly experienced in Christian cybersecurity undergraduate programs?

**RQ3.** How would a recent graduate describe, if any, whole-person skill strengths and gaps commonly experienced in Christian cybersecurity undergraduate programs?

**RQ4.** How would a recent graduate describe their cumulative experience at a Christian cybersecurity undergraduate program?

**Research Design and Methodology**

The preferred research methodology for this study was qualitative, exploratory, phenomenological research. This approach was optimal due to gaining a holistic understanding of the current satisfaction of recent graduates during analysis and evaluation of their alma mater’s cybersecurity program effectiveness. Performing a qualitative research method allows for both exploring the processes and gaining a holistic account. In the entire qualitative research process, the researchers keep a focus on learning the meaning that the participants hold about the
problem or issue, not the meaning that the researchers bring to the research or that writers express in the literature (Creswell, 2018, pp. 179-180).

This qualitative study was further refined as exploratory phenomenological research to explore and evaluate the current trends of satisfaction seen from the recent graduates of Christian cybersecurity undergraduate programs. Phenomenological studies are used by qualitative research to identify an “object” of human experience (phenomenon) that is experienced by several individuals (Creswell & Poth, 2017, p. 75). This research conducted was classified as phenomenological research as this researcher collected data from graduates who have experienced the phenomenon (undergraduate Christian cybersecurity program) and analyzed the essence of the “what” and “how” the experience was for all of the individuals (Moustakas, 1994; Creswell & Poth, 2017, p. 75).

This qualitative, exploratory, phenomenological research surveyed seven cybersecurity professionals that have graduated from a Christian undergraduate cybersecurity program within the last five years. This survey attempted to capture and analyze positive and negative trends that Christian cybersecurity programs have within their program and collegiate experience. Various research and references discuss the current skills cybersecurity professionals need to be successful in the workforce; however, this researcher made an attempt to seek those who are experiencing the fruits of their academic rigor and labor. These individuals were in an optimal position to describe their recent educational experience while discussing how their holistic educational transformation either met or missed different aspects for their employment needs.

**Setting**

The setting for this research consisted of individuals that have graduated from a US-based Christian undergraduate cybersecurity program within the last 5 years. This geographically
separated research allowed for a general view of the wide array of technical, non-technical, and whole-person needs the cybersecurity industry requires. If a specific region of the United States were to be a primary source of candidates to be interviewed (which was not the case), the needs of the cybersecurity professional may be skewed to the needs of the specific region. For example, TEKsystems (2021) reports that the top three industries that are employing cybersecurity professionals are Information Technology and Services, Financial Services, and Security and Investigations. Comparatively, the Upstate South Carolina region has Hospital and Healthcare as the top industry, followed by Financial Services, and Security and Investigations. Regional needs differ, thus a national approach offers a model more appropriate to programs targeting a more diverse range of contexts. Additionally, if the research had a high percentage of students that attended the same university (which was not the case), this research may not accurately reflect strengths or shortcomings with all Christian cybersecurity programs but just their institution alone. Data will be analyzed collectively across all programs (not individually).

The Christian colleges and universities that were selected for this qualitative, exploratory, phenomenological research will not be disclosed. Pseudonyms were used to protect the identity of the institution and to prevent an undesired and unintentional direct comparison of how well one institution is doing in preparing students versus another institution; however, the alma mater of each student will be known to the researcher to be able to identify characteristics and positive and/or negative trends that one or more institutions have. Even though the number of Christian colleges and universities that have had cybersecurity graduates in the workforce for the past five years is relatively low, the identity of the institutions will remain masked to the reader and fellow cybersecurity program directors and/or leaders of the other programs that were evaluated.
This researcher reached out to various Christian cybersecurity undergraduate leaders to gain approval to reach out to their graduates that are in the workforce. This researcher reached out to these educational leaders via an initial email and a follow-up email to briefly describe the desired research that was going to be performed and requested institutional approval for this research to measure their program’s effectiveness via their recent graduates. This researcher was prepared to bypass educational leader support and solicit participants directly if educational leaders did not respond to this researcher’s request. This preparation was helpful as this researcher was unable to gain support from multiple leaders of Christian institutions that offer a cybersecurity undergraduate program.

This researcher planned to use the participating educational leaders as an expert panel to review the survey; however, this expert panel was unable to occur due to not gaining educational leader support. The educational leaders would have had the opportunity to review and provide input to the survey prior to the graduates receiving the survey. This approach would have provided additional validity and allowed the participating educational leaders to identify any gaps that may have been missed during this researcher’s development of the survey. The Permission Request and Invitation to Expert Panel Letter that was utilized in an attempt to gain educational leader support is located at Appendix D. The Permission Letter that was also utilized in an attempt to gain educational leader support is located at Appendix E.

Once this researcher would have gained approval from the educational leaders, each educational leader would have had the opportunity to review and offer any input to the survey questions, and gained approval to reach out to their graduates. This researcher would have provided each potential respondent with information about the study and a link to a survey.
Due to not gaining educational leader support, this researcher identified potential participants via social media and other networking means. The researcher introduced himself and sent a link that included an informed consent disclosure and the opportunity to take or decline to take the survey. The survey asked various qualitative questions regarding their technical, non-technical, and whole-person development they experienced at their institution and the participant's satisfaction with the preparation they received to enter the workforce. The survey link, collection, and methodology assisted with keeping the identity of the participants and institutions hidden.

**Participants**

For a participant to have been eligible for this research, the following criteria must have been met:

- The participant must have graduated with a four-year degree in cybersecurity (or similar e.g., information security, computer security, etc.) from a Christian institution.

- The participant must have been employed full-time in the workforce no more than five full years after graduation. The purpose of no more than five years is intended to ensure the student has not had one or more years in the workforce than the typical four-year college journey. Analyzing a cybersecurity professional with more than five years of experience may indirectly result in analyzing the student’s development while on-the-job, rather than during their collegiate career.

- The participant must be currently employed in a cybersecurity role.

Once the graduates met these requirements and were interested in participating in the survey, they received an anonymous link. Within this survey, there was a Consent Form (Appendix F) and a questionnaire reconfirming they met all of the criteria above. Once they reconfirmed their qualifications to participate, participants were provided with a variety of questions describing their satisfaction with the holistic preparation they received at their institution. These questions were broken down into three transparent categories that were
known to the participants; technical, non-technical, and whole-person.

The technical category collected data pertinent to their preparation to perform technical cybersecurity tasks. Technical cybersecurity tasks included but were not limited to: cryptography; networking; network defense; scripting; and hacking.

The non-technical category collected data pertinent to their preparation to perform non-technical cybersecurity tasks. Non-technical cybersecurity tasks included, but were not limited to: cybersecurity planning and management; policy, legal, ethics, and compliance; security risk analysis; and cyber threats.

The whole-person category collected data pertinent to the non-cybersecurity-related skills and traits they developed at their institution. Whole-person traits included, but were not limited to: love; strength; steadfastness; faithfulness; and being on guard. The participants responded to this survey by freely expressing their experiences with essay entry options instead of Likert-style questions. The final question of each of these three was an open-ended question to allow the participant to share any additional insight.

Upon completing the whole-person stage of the survey, they were provided with an essay request to describe their cumulative experience in 125-250-words. Upon completing the survey, they received a page thanking them for their participation and confirming their survey has been collected. This page also provided them with this researcher’s contact information if they have any questions in the future and means to collect their compensation in an anonymous manner.

**Role of the Researcher**

“Good qualitative researchers take certain precautions to enhance the trustworthiness and credibility of their findings” (Leedy & Ormand, 2018, p. 356). Leedy and Ormand went on to say
that the qualitative researcher must strive for balance, fairness, completeness in data analysis and interpretation, carefully document information, and be upfront about personal biases (p. 356-357). Since the researcher is a full-time faculty member teaching cybersecurity at a new Christian cybersecurity program, special consideration is required to ensure personal biases did not affect the research. The researcher’s program was not be included in the study and due care was necessary to ensure the personal style and preferences of the researcher did not inappropriately impact how the information is processed. It should be noted that this researcher did not have any cybersecurity graduates from his institution’s new cybersecurity program during the time of this research.

The role of this researcher in this qualitative, exploratory, phenomenological research was to adequately gain and analyze data regarding the technical, non-technical, and whole-person development and preparation students received during their four-year undergraduate cybersecurity program journey at a Christian institution. This researcher did not have any known conflict of interest nor bias towards the selection of the participants as this researcher did not personally know any of the respondents prior to the completion of their survey responses. This researcher also did not personally know any of the program directors that were surveyed in this research. To protect against bias towards the effectiveness of these institutions and this researcher’s influence on how the participants respond to the survey, the researcher provided each participant with a survey that securely collected, transported, and secured their responses. This uniformity, as compared to a one-on-one interview or focus group discussions, ensured that each participant had identical questions, wording, and influence of the researcher’s questions as the other participants of all institutions. Performing live dialogue with the participants when interviewing and collecting data could have led to indirect influence on the student’s satisfaction
and reporting with their alma mater that may differ from this researcher’s pre-determined opinions through natural direct and in-direct dialogue.

The Institutional Review Board (IRB) proposal was submitted to the Liberty University IRB due to the intended utilization of questionnaires and surveys and how the interviews and observations were to be conducted in this research (Roberts, 2010; Jackson, 2020). Roberts (2010) stated that the main purpose of an IRB is to ensure the “protection of those participating in the research study, particularly around ethical issues such as informed consent protection from harm, and confidentiality” (p. 200).

**Ethical Considerations**

Ethical considerations arise in every aspect of conducting research, including the “attention to human rights, data collection, data analysis, and data interpretation, respect for the research site, writing, and disseminating the research” (Roberts, 2010, p. 200). There is the presence of the customary guidelines to include “protection from harm, voluntary and informed consent, and the participant's right to privacy, and honesty with professional colleagues” (Leedy & Ormond, 2018, p. 111).

One ethical consideration is the potential disclosure of information that could harm either the participant (graduate), their alma mater’s cybersecurity program, or both. This researcher agreed to the following terms with the participants to gain trust in the research process:

- The records of this study will be kept private
- Published reports will not include any information that will make it possible to identify a subject
- Research records will be stored securely, and only the researcher will have access to the records.
- Data collected may be shared for use in future research studies or with other researchers.
• If the data collected is shared, any information that could identify you, if applicable, will be removed before the data is shared.

• Institutions will be assigned a pseudonym. I will conduct the research and analysis where others will not be able to view the unprotected data.

• Data will be stored on a password-locked computer and may be used in future presentations. The data will be backed up to two external hard drives. Any paper documentation will be protected in a code-protected, fireproof safe.

Another ethical consideration is that this researcher is currently a full-time faculty member at a Christian college that is providing cybersecurity education. It is vastly important other institutions trust that their own institution was not being analyzed by a competitor in the higher education industry, but a friend and colleague that shares the same values of providing optimal education for their students. This data is now freely available for researchers to gain access to and learn from.

Data Collection Methods and Instruments

This section provides a brief description of the data the researcher searched for to answer the research questions, the reasoning for selecting this data type, and pinpoints the sought-out data for this research design. This qualitative, exploratory, phenomenological research utilized online surveys as the method of data collection to have the lowest amount of researcher influence. The questionnaire instrument was developed and consisted of 47 questions across five different portions of the research (participant qualification, technical, non-technical, whole-person, and cumulative). Lastly, the procedures and approvals (including IRB) required for data collection are discussed below.

Collection Methods

Utilizing Jackson’s (2020) research of a multi-case qualitative study of servant leadership in a specific region, this researcher compared Jackson’s definitions of four different approaches for a qualitative case study and selected surveys as the data collection method that is ideal for
this specific research and ethical considerations. Surveys, compared to interviews, focus groups, and observation, were the method with the lowest influence and disruption by the researcher. Surveys are “high level of structure and standardization, commonly used to collect data from large numbers of people, researcher involvement with the participants is low” (Jackson, 2020, p. 125). Due to the researcher bias and/or involvement being high for qualitative research that utilizes interviews, focus groups, or observations, this researcher solely utilized surveys to protect against researcher bias and influence that could have tainted the perception and quality of this research. This researcher utilized these surveys to eventually distribute, collect, and analyze the satisfaction of cybersecurity graduates of four-year Christian institutions from a technical, non-technical, and whole-person vantage point. This researcher, with experience as a cybersecurity professional and educator, utilized interviews to gain high trust in the data as to not be tainted by this researcher. The research data is slated to be openly available to Christian higher education institution cybersecurity leaders to assist with any strengths or weaknesses found during the survey.

**Instruments and Protocols**

An identical digital survey that included the Consent Form, questionnaire, qualitative questions, and responses was provided to each participant in this qualitative, exploratory, phenomenological research. The survey sought to obtain years in the workforce (after graduation), alma mater, current job role, industry of current company, satisfaction with current role (to better identify if the graduate has yet reached the desired position sought after), and the strengths and gaps experienced, if any, during their undergraduate journey across technical, non-technical, and whole-person vantage points. This survey was flexible and allowed participants to freely express their experiences with open-ended response options instead of Likert-style
questions. The survey included a total of 47 questions in five sections. The first section was the qualification portion, composed of six questions, and included verifying the participant met eligibility requirements for participating and completing the rest of the survey. The second section was the technical portion, composed of thirteen questions, and addressed the satisfaction, strengths, and gaps experienced by the participant at their alma mater during their undergraduate cybersecurity program journey. The technical categories that were utilized to create these questions were drawn from the National Security Agency’s (NSA) Center of Academic Excellence (CAE) technical and optional Knowledge Units (KUs). These KUs can be found in Appendix A (technical) and Appendix C (optional). This section answered Research Question #1 “How would a recent graduate describe, if any, technical strengths and gaps commonly experienced in Christian cybersecurity undergraduate programs?” The third section was the non-technical portion, composed of thirteen questions, and addressed the satisfaction, strengths, and gaps experienced by the participant at their alma mater during their undergraduate cybersecurity program journey. The non-technical categories utilized to create these questions were drawn from the National Security Agency’s (NSA) Center of Academic Excellence (CAE) technical Knowledge Units (KUs). These KUs can be found in Appendix B (non-technical) and Appendix C (optional). This section answered Research Question #2 “How would a recent graduate describe, if any, non-technical strengths and gaps commonly experienced in Christian cybersecurity undergraduate programs?” The fourth section was the whole-person portion, composed of fourteen questions, and addressed the satisfaction, strengths, and gaps experienced by the participant at their alma mater during their undergraduate cybersecurity program journey. The whole-person questions and traits were pulled from Scripture and included, but were not limited to: love; strength; steadfastness; faithfulness; and being on guard (Philippians 4:8,
Matthew 5:8, 1 Timothy 4:12 1 Corinthians 6:13-14). This section answered Research Question #3 “How would a recent graduate describe, if any, whole-person skill strengths and gaps commonly experienced in Christian cybersecurity undergraduate programs?” The fifth, and final, section consisted of one question regarding the participant's cumulative experience. The participant was asked to describe this in 125-250-words. This section answered Research Question #4 “How would a recent graduate describe their cumulative experience at a Christian cybersecurity undergraduate program?”

Procedures

Eliciting participants

Prior to reaching out to eligible participants, this researcher identified potential Christian colleges in the United States that offer an in-person cybersecurity (or similar degree) four-year degree and had graduates currently in the workforce. Upon gathering potential colleges that could have supported this research, this researcher attempted to contact and share this research method with each director (or similar decision-maker) of each college via email. This researcher attempted to ensure that the fellow directors trust that this research is not being analyzed by a competitor in the higher education industry, but a friend and colleague that shared the same values of providing optimal education for their students, and this data would be freely available for all to gain access to and learn from. This researcher reached out to various Christian cybersecurity undergraduate leaders to gain approval to reach out to their graduates that are in the workforce. This researcher reached out to these educational leaders again via a follow-up email to briefly describe the desired research that was going to be performed and requested institutional approval for this research to measure their program’s effectiveness via their recent graduates. The elicitation of eligible participants was intended to begin by reaching out and
potentially meeting with directors (or equivalent decision-makers) of undergraduate
cybersecurity programs at Christian colleges and universities across the United States. The intent
of this meeting was aimed to gain their trust and support, in order to gain institutional approval to
participate and request that they contact their recent graduates (past five years) about this
research. This researcher provided the director with a fixed invitation to send to their graduates.
This researcher was prepared to bypass educational leader support and solicit participants
directly if educational leaders did not respond to this researcher’s request (which occurred). No
meetings were scheduled with directors. Due to not gaining director support from multiple
institutions, this researcher identified 46 potential participants that appeared to meet the
following eligibility based on social media and other networking means:

1. The participant must have graduated with a four-year degree in cybersecurity
   from a Christian institution. Similar degrees (e.g., information security,
   computer security, etc.) will be acceptable.

2. The participant has been employed full-time in the workforce for at least three
   months and no more than five full years after graduation.

3. Currently employed in a cybersecurity role. Graduates that have forgone a full-
   time cybersecurity role to pursue other options (e.g., different degree, graduate
   cybersecurity degree, etc.) will not be considered, unless they are also currently
   employed full-time in a cybersecurity role as well.

On November 19, 2021, the researcher introduced himself via social media and other
networking means and sent a link that included an informed consent disclosure and the
opportunity to take or decline to take the survey. The survey asked various qualitative questions
regarding the technical, non-technical, and whole-person development they experienced at their
institution and the participant's satisfaction with the preparation they received to enter the
workforce. The survey link, collection, and methodology assisted with keeping the identity of the
participants and institutions hidden. The participants were elicited and rewarded with a $25 Visa
Gift Card upon successful completion of the survey that were either be emailed or physically
mailed to them. This researcher initially aimed to solicit a minimum of 12 responses. After one week, this researcher reached out to each potential participant that did not participate yet and attempted to solicit their participation. After a total of two weeks, the survey had 94 total visits, seven completed surveys, and three additional started, but incomplete, surveys. This researcher closed the survey on December 3, 2021, as all means of soliciting participants to partake in the survey appeared to have been exhausted.

**Steps in gathering and recording the data**

The process of this qualitative, exploratory, phenomenological research was initially planned as follows:

1. Contact Directors (or equivalent decision-makers) of cybersecurity programs at Christian colleges and universities across the United States regarding the study

2. Schedule and meet with Directors one-on-one via Zoom and discuss the study more in-depth and their role

3. Upon agreeing to support their graduates in taking this research, provide these leaders with steps on a fixed message to send out to their cybersecurity graduates of the past five years

4. Upon reaching and gaining approval from a minimum of three Directors, open the survey up for participants

5. Close survey once 12-30 eligible participants have completed the survey

6. Collect the survey submissions

7. Securely store the survey submission utilizing multiple encrypted hard drives

The adapted process of this qualitative, exploratory, phenomenological research, due to not gaining director support and only identifying 46 potential participants was as follows:

1. Identified potential participants using social media and other networking means

2. Reached out to each potential participant and shared an invitation that explained the research and provided a link to the survey

3. Communicated with potential participants that responded via social media and other networking means to gain their confidence and answer any questions
4. After one week, reached out to potential participants that did not take the survey

5. After another week (two total weeks), closed the survey after the researcher exhausted all means of soliciting participants to partake in the survey

6. Collected the survey submissions

7. Securely stored the survey submission utilizing multiple encrypted hard drives

Data Analysis

This section discusses how the researcher collected and analyzed the data required to answer the research questions for this qualitative, exploratory, phenomenological research.

Analysis Methods

This researcher created a secure Zoho survey that encrypted the participant responses. The researcher distributed the surveys via an encrypted Zoho link. The researcher then transported and imported the data from an encrypted Zoho document to his local laptop and performed manual content analysis as well as utilizing the Zoho sentiment analysis. The content collected and analyzed was entirely performed utilizing this method as no audiovisual data or other observations were collected. Qualitative data was collected and analyzed for each of the participants. This analysis included comparing and contrasting their responses with the responses of the other participants to potentially identify trends of strengths and/or gaps the participants believe they experienced during their Christian cybersecurity undergraduate program journey. The researcher looked for trends that speak positively or negatively regarding technical, non-technical, and/or whole-person development and if any conclusions can be determined to help enlighten current Christian cybersecurity program directors and leaders to self-assess if they see these strengths and/or weaknesses in their own institution and program. This exploratory qualitative research method utilized the data analysis flow chart as described by Creswell (2018, p. 193) as seen in Figure 6.
Upon the survey concluding after meeting the required thresholds described above, this researcher gathered the raw data (survey responses and any applicable communication from respondents), validated the data was accurately documented and participant met eligibility, and organized the responses based on each question. For example, each response to a specific whole-person question was grouped together with the other participants’ responses to the same question. This researcher also randomized the order of each participant’s responses to each question to further anonymize and avoid a specific order of reviewing the responses from specific participants. Upon validating each respondent’s response was accurately recorded and each respondent met the eligibility requirement, this researcher read and become familiar with the responses. This ensured that no outliers, incorrect documentation, or ineligible data were present in the data that was being prepared for coding and eventual interpretation. Reviewing the responses was the initial inclination of the overall satisfaction of those that responded to the
survey and began. This researcher also ensured that multiple institutions were represented in a fairly even distribution. Furthermore, this researcher gathered definitions and identified any themes to assist with developing data for further analysis and eventual interpretation. Lastly, the researcher interpreted the themes found in the research and yet again validated the entire process of the research was valid. This final stage was supported by appropriate tables and figures to improve the readability and understanding of the strengths and gaps within the experiences of the participants interviewed.

**Trustworthiness**

In qualitative research, the standard that is most frequently used is trustworthiness. A critical evaluation of the research is required (Jackson, 2020). In this section, the researcher discussed the multiple efforts integrated into this research study to ensure the research and supporting data are worthy of trust amongst the readers of this research. Arguably, the largest threat to trustworthiness to this research was the researcher’s bias towards the survey and results due to the researcher being a faculty member of a new Christian cybersecurity undergraduate program. If this bias was not minimized and transparently addressed, the research may appear to be an attack on other institutions regarding how they should alter their program to be more aligned with this researcher’s curriculum. Creswell (2018) recommends the following:

> Clarify the bias the researcher brings to the study. This self-reflection creates an open and honest narrative that will resonate well with readers. Reflexivity has already been mentioned as a core characteristic of qualitative research. Good qualitative research contains comments by the researchers about how their interpretation of the findings is shaped by their background, such as their gender, culture, history, and socioeconomic origin. (p. 200)

To further improve the trustworthiness of the data, the definitions and questions during the survey and the analysis used rich and thick descriptions. When qualitative researchers provide detailed descriptions of the setting, for example, or offer many perspectives about a
theme, the results become more realistic and richer. This procedure Creswell discussed added to the validity of the findings (Creswell, 2018, p. 200).

Lastly, the researcher presented the negative information that may not support the overall themes (Creswell, 2018, p. 200). For example, the majority of participants were not fully satisfied with their technical experience; however, this researcher ensured to showcase all results to highlight the few that did not support the overall gap identified. This negative data assisted with ensuring the readers the data utilized for the analysis is real and so varies from participant to participant. Most evidence built a case for the theme; however, researchers can also present information that contradicts the general perspective of the theme.

**Credibility**

The credibility of this research is highlighted by the raw responses each of the participants provided to each question. All participants were given the same question. The interaction between the researcher and the participant was solely performed via electronic communication solicitation and the survey questions themselves. Communication between this researcher and the participants can be anonymized and provided to leaders of Christian institutions that can benefit from this research upon request to further prove the credibility of this research.

**Dependability**

The details of this research process and procedures were shared above in the *Steps in gathering and recording the data* section. These processes and procedures included the initial outline and the adapted steps after not receiving educational leaders’ support. Future researchers are able to depend on these steps to perform future research in a similar manner. Identifying unknown potential participants is highly dependent on being able to utilize social media and
other open-source resources to find people that may fit the requirements for the research. This identification process can be made easier and reach a wider audience by gaining educational leader support.

**Confirmability**

The “audit trail” to provide confirmability of the processes and procedures used to collect and interpret this data has been documented and highlighted within this research. This research showcases each of the participant’s responses scrambled to avoid publicly identifying individual responses throughout each question. Access to individual, raw responses from Zoho and further proof of the processes and procedures will be made available upon request to leaders within Christian institutions that can benefit from this research. This study was designed to create a feedback loop that spanned multiple Christian institutions and in doing so this researcher is open to defending this work and discussing this research with leaders of Christian institutions that can benefit from this research.

**Transferability**

The processes and procedures utilized in this research to collect and interpret the data can be transferred and replicated in other settings. This research was aimed towards surveying cybersecurity professionals that graduated in the last 5 years with a four-year degree in cybersecurity from a Christian institution. The following settings and target audiences could utilize the same processes and procedures utilized in this research:

- Cybersecurity professionals that graduated after August 31, 2021, with a four-year degree in cybersecurity from a Christian institution.
- Cybersecurity professionals that graduated in [any timeframe] with a graduate degree in cybersecurity from a Christian institution.
- Cybersecurity professionals that graduated in [any timeframe] with a four-year degree in a non-cybersecurity field from a Christian institution.
• Cybersecurity professionals that graduated in [any timeframe] with a four-year degree in cybersecurity from a Catholic institution.

• Cybersecurity professionals that graduated in [any timeframe] with a four-year degree in cybersecurity from a private institution.

• Cybersecurity professionals that graduated in [any timeframe] with a four-year degree in cybersecurity from a public institution.

• Cybersecurity professionals that graduated in [any timeframe] with a four-year degree in cybersecurity from [any scope of an] institution.

It should be noted that researchers that choose to utilize this research process and procedures may choose to modify the whole-person and Scripture references if the target audience and institutions do not align with these Biblical and religious beliefs.

**Chapter Summary**

The purpose of this chapter was to describe the research methodology that will be utilized for this study. This description was conducted by reviewing the research design synopsis and qualitative research methodology. The first section, research design synopsis, described the problem (unmeasured effectiveness of Christian undergraduate cybersecurity programs), purpose statement (evaluating Christian undergraduate cybersecurity programs), four research questions, and the research design and methodology. The second section delved into the research design and methodology that included the setting, participants, role of the researcher, ethical considerations, data collection methods and instruments, research instruments, and data analysis.
CHAPTER FOUR: ANALYSIS OF FINDINGS

Overview

This chapter dives into the collection and analysis of the data. First, the particular steps taken by the researcher in collecting and compiling the data is discussed to highlight the study’s research methodology and its implementation. Secondly, an analysis of the data is performed in a specific manner to address this study’s research questions.

Compilation Protocol and Measures

This section addressed the process of identifying potential participants, soliciting participants, collecting data, recording data, organizing data, and processing data. The research discusses how potential participants were identified.

Identifying Potential Participants

Each of the seven participants that partook in this anonymous survey was contacted via electronic medium. Prior to this research, the researcher did not have any contact with the anonymous participants. The researcher utilized social media sites and other online resources to identify 46 potential participants that appeared to meet the requirements for this study. The researcher individually reached out to each potential participant.

Soliciting Participants

The researcher was able to begin a discussion with 25 potential participants and attempted to share the purpose of this research, the compensation, and the recruitment letter (Appendix F). The recruitment letter contained the link to the Zoho survey. Multiple potential participants notified the researcher they did not meet a prerequisite due to either not graduating or not being in a full-time cybersecurity-related role. Ultimately, over 14 days of reaching out to
these potential participants, the researcher received 7 completed anonymous survey responses via the Zoho survey that was attached to the recruitment letter.

**Collecting Data**

An anonymous survey was the chosen approach to collect the open-ended, qualitative, anonymous data. This survey was performed via Zoho to leverage the ability to encrypt participants’ answers while the data is at-rest on Zoho’s platform, ability to export the results via TLS encryption and the document encrypted with a passphrase while the data is in-transit, and for privacy and anonymous concerns for the participants (e.g., not collect IP addresses). The Zoho link that was sent via the recruitment letter also did not contain any unique identifiers that could demask the anonymity of the participant. In other words, each participant was presented with the same link and afforded the participants the opportunity to take the survey without the researcher knowing which participants clicked the survey, if they chose to do so. All questions created for the Zoho survey had the additional ‘encrypt answer’ functionality enabled. Throughout the Zoho survey, the participants were made aware of their progress with a progress bar. The survey created for the participants contained 7 sections:

1. Consent Form
2. Qualifier
3. Qualifier Details
4. Technical Section
5. Non-Technical Section
6. Whole-Person Section
7. Cumulative Question
*Consent Form*

Each participant was presented with the Consent Form (Appendix G) as the first page of the survey and the Consent Form Agreement Question (Appendix H). If the participant did not agree to the Consent Form by selecting ‘No’, they were sent to the “Disqualification Page”. If the participant agreed to the Consent Form by selecting ‘Yes’, they were presented with the Qualifier section.

*Qualifier*

The Qualifier section contained a page explaining the requirements to partake in this survey and the Qualifier Question (Appendix I). If the participant stated they did not meet the requirements by selecting ‘No’, they were sent to the “Disqualification Page”. If the participant selected they met the requirements by selecting ‘Yes’, they were presented with the Qualifier Details section.

*Qualifier Details*

The Qualifier Details section contained the following 6 questions (Appendix J) gaining additional details to verify they meet the qualifications. This Qualifier Details section was utilized by the researcher to manually verify each participant met the qualification and would have discarded their submission if the participant did not meet the requirements. Each of these questions was mandatory to answer to continue the survey. Once the participants verified they met the requirements by answering the Qualifier Details section, they were presented with the Technical section.

*Technical*

The Technical section contained 13 questions (Appendix K) directly related to answering Research Question #1 “How would a recent graduate describe, if any, technical skill strengths
and gaps commonly experienced in Christian cybersecurity undergraduate programs?” Each of these questions was mandatory to answer to continue the survey. Once the participants completed each of these questions, they were presented with the Non-Technical section.

**Non-Technical**

The Non-Technical section contained 13 questions (Appendix L) directly related to answering Research Question #2 “How would a recent graduate describe, if any, non-technical skill strengths and gaps commonly experienced in Christian cybersecurity undergraduate programs?” Each of these questions was mandatory to answer to continue the survey. Once the participants completed each of these questions, they were presented with the Whole-Person section.

**Whole-Person**

The Whole-Person section contained 14 questions (Appendix M) directly related to answering Research Question #3 “How would a recent graduate describe, if any, whole-person skill strengths and gaps commonly experienced in Christian cybersecurity undergraduate programs?” Each of these questions was mandatory to answer to continue the survey. Once the participants completed each of these questions, they were presented with the Cumulative section.

**Cumulative**

The Cumulative section contained a question (Appendix N) directly related to answering Research Question #4 “How would a recent graduate describe their cumulative experience at a Christian cybersecurity undergraduate program?” Answering this question was mandatory; however, meeting the 125-word minimum was not mandatory. This detail was unknown to the participant unless they attempted to submit an answer that was less than 125-words. Once the
participants completed each of these questions, they successfully completed the survey and were redirected to the Survey End Page.

**Survey End Page**

The Survey End Page thanked the participants for participating in the survey and presented the participants with three options to receive their $25 Visa gift card compensation. Three compensation delivery options (Appendix O) were presented to those whom successfully completed the survey. Each participant was compensated within 2 hours of completing their survey and submitting their compensation delivery choice. The participants that contacted the researcher after completing the survey via email, text, or other messaging were yet again thanked for their participation and were asked to share the recruitment letter with additional potential participants, if they wanted to. No completed surveys were submitted by participants that were not initially solicited by this researcher. In other words, no participant successfully recruited others to partake in this research.

Upon closing the survey link, the researcher exported the survey responses as encrypted, password-protected .csv files. The researcher validated that each of the 7 surveys was successfully exported and each of the questions included 7 responses. Next, the researcher verified that each participant completed the Consent Form and verified they met the requirements of this study. Upon verifying each participant completed the required pre-requisites, the researcher, utilized Kutools for Excel, to randomly scramble the order of the responses in Excel to remove any direct relationships to further anonymize the responses across different questions. The researcher tested Kutools for Excel’s randomization functionality against the 7 responses for the first 5 questions and verified Kutools for Excel randomized the responses to remove any direct links to a particular participant’s responses across multiple
questions. The researcher scrambled the 7 responses for all 47 questions. The researcher then validated that each of the 47 questions had 7 accurate responses.

The researcher then read through each of the 6 questions and responses within the Qualifier Details section. The researcher identified one participant who responded they were in the workforce for “3” and did not identify whether it was 3 months or 3 years. The researcher was able to verify this participant has been in the workforce for roughly 3 years after graduation. The researcher verified the year the student graduated, the institution they graduated from, and their current employment details all met the requirements for this research.

The researcher read through each of the 13 questions and responses within the Technical section. No glaring clarification issues were found within the Technical section by the researcher. The researcher read through each of the 13 questions and responses within the Non-Technical section. No glaring clarification issues were found within the Non-Technical section by the researcher. The researcher read through each of the 14 questions and responses within the Whole-Person section. No glaring clarification issues were found within the Whole-Person section by the researcher.

Furthermore, the researcher read through the Cumulative section which contained 1 question that asked for a 125-250-word essay. No glaring clarification issues were found within the Cumulative section by the researcher; however, it appeared that multiple responses did not directly address the question.

Before analyzing the data, the researcher sanitized the data by replacing any mention of institutions’ names with their pseudonym. The researcher also sanitized the data by generalizing any specific details that could demask the anonymity of the participants. Any utilization of parenthesis and italics (e.g., (pentester/red team)) indicates the researcher sanitized the data for
anonymity purposes. The researcher also normalized the data by capitalizing the first word of each sentence as one participant commonly left the first character lowercase (thus easily identifying response correlation between questions).

Lastly, any confusing word structure was modified to include an italicized question mark inside a parenthesis (e.g., (??)) to highlight the confusing wording. All other wording or improper grammar was left unchanged to maintain the integrity of the data being sampled.

**Demographic and Sample Data**

**Demographics**

As discussed previously, this research is delimited to only private colleges that are members of the Council for Christian Colleges & Universities (CCCU), recognized as a Creation College by Answers in Genesis, and/or a Protestant Christian institution by viewing their website and/or mission/faith statement(s) and the institution must have a brick-and-mortar presence and be headquartered in the United States of America. Two institutions were represented by the 7 participants that completed this survey. These institutions will be assigned the pseudonyms Christian College A and Christian College B. Table 5 shows Christian College A had 3 participants while Christian College B had 4 participants. It should also be noted that Christian College A and Christian College B are located in different states, have no official relationship with each other, and are their own distinct Christian college or university that met this research’s delimitations.
Table 5

Participants' Institution

<table>
<thead>
<tr>
<th>Institution Pseudonym</th>
<th>Number of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Christian College A</td>
<td>3</td>
</tr>
<tr>
<td>Christian College B</td>
<td>4</td>
</tr>
</tbody>
</table>

This research is also delimited to participants who have graduated with a four-year degree in cybersecurity (or similar field, e.g., information security, computer security, etc.) from a Christian institution that meets the above requirements. Table 6 shows that 100% of participants, regardless of which institution they attended, received a Bachelor of Science degree in Cybersecurity.

Table 6

Participants' Degree

<table>
<thead>
<tr>
<th>Degree</th>
<th>Number of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>BS in Cybersecurity</td>
<td>7</td>
</tr>
</tbody>
</table>

Furthermore, this research was delimited to participants who have been employed full-time in the cybersecurity workforce no more than five full years after graduation and are currently employed in a cybersecurity role. Table 7 shows the year each participant graduated.

Table 7 showcases a 0% participation rate from professionals that graduated between 2016-2018. Table 7 showcases 100% of participants of this research graduated between 2019-2021. The majority (4 participants) graduated in 2021, while 2 participants graduated in 2020 and 1 participant graduated in 2019.
Table 7

Participants' Graduation Year

<table>
<thead>
<tr>
<th>Graduation Year</th>
<th>Number of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>0</td>
</tr>
<tr>
<td>2017</td>
<td>0</td>
</tr>
<tr>
<td>2018</td>
<td>0</td>
</tr>
<tr>
<td>2019</td>
<td>1</td>
</tr>
<tr>
<td>2020</td>
<td>2</td>
</tr>
<tr>
<td>2021</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 8 shows the responses regarding how long they have been in the cybersecurity workforce. The majority (4 participants) have been in the workforce for 6 months or less. 2 participants have been in the workforce for about 1 year (11 months or 1 year). Lastly, 1 participant claims to have been in the workforce for 3 years since graduation. Table 8’s time in the workforce supports the findings of Table 7’s graduation year.

Table 8

Participants' Time in Workforce

<table>
<thead>
<tr>
<th>Time in Workforce</th>
<th>Number of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 months</td>
<td>2</td>
</tr>
<tr>
<td>4 months</td>
<td>1</td>
</tr>
<tr>
<td>6 months</td>
<td>1</td>
</tr>
<tr>
<td>11 months</td>
<td>1</td>
</tr>
<tr>
<td>1 year</td>
<td>1</td>
</tr>
<tr>
<td>3 years</td>
<td>1</td>
</tr>
</tbody>
</table>
This research requested the industry and current work performed to highlight the diversity of current job roles each participant currently possesses. Participants were asked how their experience relates to their current job role. Table 9’s details have been stripped and generalized to preserve the anonymity of the participants as specific keywords, job titles, or industries could unintentionally reveal the identity of the participants. Table 9 highlights that 5 participants appear to be in a technical cybersecurity role (3 Cybersecurity/SOC Analysts, 1 DoD Contractor (Engineer), and 1 IT/Financial). Table 9 also highlights 1 participant is in a non-technical role (Risk Management/Consultation) and the technical or non-technical role was unable to be identified for 1 participant (DoD Contractor (No details)).

Table 9

Participants' Current Work

<table>
<thead>
<tr>
<th>Industry and/or Title</th>
<th>Number of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity/SOC Analyst</td>
<td>3</td>
</tr>
<tr>
<td>DoD Contractor (Engineer)</td>
<td>1</td>
</tr>
<tr>
<td>DoD Contractor (No details)</td>
<td>1</td>
</tr>
<tr>
<td>Risk Management/Consultation</td>
<td>1</td>
</tr>
<tr>
<td>IT/Financial</td>
<td>1</td>
</tr>
</tbody>
</table>

This research requested the satisfaction of the participant regarding their current cybersecurity-related work role. Table 10 showcases 4 participants responded extremely positively (“Love it” or “Highly/Very Satisfied”), 2 participants responded positively (“Satisfied”), and 1 participant responded with “Mildly Satisfied”. Table 10 showcases all participants indicated they are satisfied in some capacity with their current work role.
Table 10

Participants' Work Role Satisfaction

<table>
<thead>
<tr>
<th>Satisfaction Level</th>
<th>Number of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Love it” or “Highly/Very Satisfied”</td>
<td>4</td>
</tr>
<tr>
<td>“Satisfied”</td>
<td>2</td>
</tr>
<tr>
<td>“Mildly Satisfied”</td>
<td>1</td>
</tr>
</tbody>
</table>

Data Analysis and Findings

This section will share the results and analyze the results of the participants regarding their technical section responses, non-technical sectional responses, whole-person responses, and cumulative responses. This section will also attempt to find trends between the 7 participants specific to each of the research questions.

Research Question #1

As stated previously, the Technical section contained the following 13 questions directly related to answering Research Question #1 “How would a recent graduate describe, if any, technical skill strengths and gaps commonly experienced in Christian cybersecurity undergraduate programs?”. The following 13 tables (Table 11 – 23) showcase the responses to the 13 questions asked in the Technical section of the survey. These questions will be labeled T.1 through T.13.

Question T.1 requested the participant’s satisfaction regarding the technical knowledge and skills learned from their institution. Table 11 showcases that 2 participants responded positively with either “Yes” or “Satisfied”. It also showcases that 2 participants responded with “Mildly Satisfied” or “Somewhat Satisfied”. Table 11 continues by showcasing 1 participant
responded with “Not Fully Satisfied”. Lastly, Table 11 showcases 2 participants responded with “Not Really” or “No”.

Table 11

*Overall Technical Satisfaction*

<table>
<thead>
<tr>
<th>Technical Satisfaction Level</th>
<th>Number of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Yes”/“Satisfied”</td>
<td>2</td>
</tr>
<tr>
<td>“Mildly/Somewhat Satisfied”</td>
<td>2</td>
</tr>
<tr>
<td>“Not Fully Satisfied”</td>
<td>1</td>
</tr>
<tr>
<td>“Not Really”/“No”</td>
<td>2</td>
</tr>
</tbody>
</table>

Question T.2 requested the participants to go into further detail explaining their satisfaction regarding the technical knowledge and skills learned from their institution. Table 12 showcases the participants' responses. Zoho’s sentiment analysis indicated 3 participants responded with disappointed sentiment, 2 participants responded with neutral sentiment, 1 participant responded with happy sentiment, and 1 participant responded with extremely happy sentiment. Zoho’s sentiment analysis can be found in Figure 7. Table 12 showcases 6 participants responded in a manner that described a desire for the institution to provide more technical knowledge and skills or highlighted the institution taught minimal technical knowledge and skills. Only 1 participant responded in a manner that did not describe a desire for the institution to provide more technical knowledge and skills.
Table 12

*Overall Technical Satisfaction Detailed*

(T.2) Please describe in more detail your satisfaction level with the technical knowledge and skills your institution helped you develop.

“I am happy with the information, knowledge, and insights that I learned at Christian College A”

“I wish more of the homework assignments were labs instead of studies.”

“Christian College B did a good job describing the tech knowledge needed but could have spent more time on skills.”

“I really feel only a few classes actually prepared me for what I am doing now.”

“I was left wishing that my program had focused more on teaching us students some of the technical skills that are very prevalent within InfoSec. A lot of the time there would be a lecture but no substance to actually apply the information that had been taught. A large area which I wish was covered more is Networking and trouble shooting.”

“Once I began by career, I realized just how much I did not know coming out of school. I also had used self-learning platforms (TryHackMe, Hack the Box) which gave me lots of practical knowledge I would not have had, had I solely relied on my college courses.”

Figure 7

*Sentiment Analysis of Overall Technical Satisfaction Detailed Responses*

![Sentiment Analysis Chart]

42.86%  28.57%  14.29%  14.29%

Question T.3 requested the participants to discuss if their institution spent more time teaching technical knowledge or technical skills. Table 13 showcases the participants’ responses. Table 13 showcases 5 participants explicitly stated more time was spent teaching technical knowledge. 1 participant stated “hands-on technical knowledge”; however, the hands-on adjective indicates this participant may have intended to respond with hands-on technical skills. This participant’s response was not aggregated as 1 of the 5 participants explicitly stated more
time was spent teaching technical knowledge. 1 participant responded with a scenario of how faculty would teach hands-on skills; however, did not directly answer the question.

Table 13

**Technical Knowledge or Skills**

<table>
<thead>
<tr>
<th>(T.3) Please describe if your institution spent more time teaching cybersecurity technical knowledge or technical skills. Please describe how this time was spent.</th>
</tr>
</thead>
<tbody>
<tr>
<td>“We did more knowledge. There was a lot of book knowledge type information, and there weren't as many labs as there should have been. And the ones that we were given were all guided, so it didn't force us to learn, outside of my pentesting classes, which were just electives.”</td>
</tr>
<tr>
<td>“Some of my professors would sometimes organize an event centered around the National Cyber League, and would walk students through how to do some of the exercises. I felt as though these exercises really helped me have a better grasp on some of the technical skills within InfoSec.”</td>
</tr>
<tr>
<td>“More time on knowledge. Time was spent through textbooks and online discussion boards.”</td>
</tr>
<tr>
<td>“When I was there, more time was spent teaching the technical knowledge.”</td>
</tr>
<tr>
<td>“I would say more time was spent teaching knowledge. This time was spent through classroom lectures.”</td>
</tr>
<tr>
<td>“It depended on the teacher but a lot of them made heavy use of labs to give hand-on knowledge (skills?) of what we were learning.”</td>
</tr>
<tr>
<td>“My institution spent more time teaching technical knowledge. We had some labs to complete for practical use/skills, but most where not up-to-date or intriguing. Knowledge came from textbooks and labs / a course in the TestOut platform. Our institution was in the beginning stages of a cyber range, but I was only able to utilize it twice, which resulted in minimal learning. Most classes learned towards self-teaching, so you would get out what you put in.”</td>
</tr>
</tbody>
</table>

Question T.4 requested the participants to discuss any strengths regarding the technical knowledge and skills they developed at their institution. Table 14 showcases the participants' responses. Table 14 showcases 2 participants indicated the knowledge of the professors and/or staff as a strength of the institution regarding technical knowledge and skills. Table 14 also showcases 2 participants indicating that certifications (e.g., Security+) as a strength. It also
showcases 2 participants responded that no technical strengths were encountered at their institution. CTFs and ethics were also listed as a technical strength for 1 participant each.

**Table 14**

*Technical Strengths*

<table>
<thead>
<tr>
<th>(T.4) Please describe any strengths at your cybersecurity program, if any, regarding the technical knowledge and skills your institution helped you develop.</th>
</tr>
</thead>
<tbody>
<tr>
<td>“The TestOut course provided knowledge that was comparable to information on the CompTIA Security+ exam. I was also able to compete in the Cyber Skyline NCL games, a CTF tournament for college students. I learned a lot through the CTF, from using Linux to ciphers and OSINT. These were the most memorable/beneficial items from my college cyber experience.”</td>
</tr>
<tr>
<td>“Our primary strength is the importance that Christian College A puts on Ethics. This makes for good clean slates that will make good choices in the work environment, hopefully.”</td>
</tr>
<tr>
<td>“Unfortunately, nothing regarding technical skills at my university stood out. I learned most of what I know, from a technical standpoint, at Community College.”</td>
</tr>
<tr>
<td>“I would say a strength of the program was the knowledge of the staff and how much they cared about our success.”</td>
</tr>
<tr>
<td>“The best thing is that the program teaches based on certifications (A+, Network+, Security+, PenTest+, etc.)”</td>
</tr>
<tr>
<td>“Can't think of any.”</td>
</tr>
<tr>
<td>“Knowledge of the professors was a definite strength.”</td>
</tr>
</tbody>
</table>

Question T.5 requested the participants to discuss any gaps regarding the technical knowledge and skills they developed at their institution. Table 15 showcases the participants' responses. Table 15 showcases 4 participants indicated a gap with technical skills (e.g., Linux, networking, labs were too easy). 1 participant was unable to identify a gap within the technical knowledge and skills developed at the institution. 1 participant indicated the lack of encouraging students to pursue certifications as a technical gap. 1 participant indicated there just is not enough time to learn everything in the four years at school.
Table 15

*Technical Gaps*

(T.5) Please describe any gaps at your cybersecurity program, if any, regarding any technical knowledge and skills you may not have developed.

“Could have spent more time on hands on technical skills.”

“Can't think of any gaps.”

“There was not a lot of teaching on Linux usage, most of this I had to discover for my self. There also were not many Cyber Ops skills gained from college courses (think PenTesting, Threat Hunting, SOC).”

“The gaps would definitely be within the Networking classes, and the hands on experience there. Not once did a professor show us how to log into a server via PuTTY or configure a switch/ router. The most that was accomplished in those classes is to run simple Ping commands in the Windows Command line.”

“As mentioned before, all the labs didn't represent real world problems very well at all. They are too easy and were too closed ended, and walking through a lab together doesn't teach students very much.”

“Idk if I would say this is a gap, but just from the classroom limitations, the professors can only teach us so much. In cybersecurity there is so much information to learn and only so much can be taught in your time at school.”

“I would have encouraged students to get certs more than just present generic tests and quizzes.”

Question T.6 requested the participants to discuss their satisfaction regarding the technical knowledge and skills they developed at their institution as it relates to their current job role and industry. Table 16 showcases the participants’ responses. Table 16 showcases 3 participants responded negatively, 3 participants responded positively, and 1 participant responded with “minimally satisfied”.
Table 16

Technical Satisfaction Related to Work Role

(T.6) Are you satisfied with the technical knowledge and skills your institution helped you develop as it relates specifically to your current job role and industry?

“I am minimally satisfied.”
“No”
“Yes.”
“Satisfied”
“Yes I am satisfied”
“Nothing I did in school relates to my job now.”
“Not necessarily.”

Question T.7 requested the participants to go into further detail explaining their satisfaction regarding the technical knowledge and skills they developed at their institution as it relates to their current job role and industry. Table 17 showcases the participants’ responses. Table 17 showcases 2 participants responded in a negative manner by discussing the technical knowledge and skills were lacking or more time developing hands-on skills would have been preferred. The remaining 5 participants responded in a positive manner regarding technical knowledge and skills related to their current job role and industry.

Table 17

Technical Satisfaction Related to Work Role Detailed

(T.7) Please describe in more detail your satisfaction level with the technical knowledge and skills your institution helped you develop as it relates specifically to your current job role and industry.

“Due to involvement in GRC, I did not need in-depth technical skills in my current role. The ones I do have, certainly benefit me, but they would not be required to be competent in the role.”

“Since I am (a pentester/red team), the program really taught me how to think like a hacker.”
“I still have a ton to learn, but at least they gave me the tools that are necessary for me to grasp basics about information security tools, so that I am fairly versatile as a fresh Cybersecurity graduate.”

“I would have preferred my school had spent more time developing hands on skills to make the transition into the working world easier.”

“Technical knowledge is pretty good.”

“They knowledge and skills obtained from school really helped me to jump into my job with a grasp of the cybersecurity landscape.”

“I learned to be more analytical at my institution and how to notice trends in information more easily, but other than that I feel as it were lacking.”

Question T.8 requested the participants to discuss if their institution spent more time teaching technical knowledge or technical skills as it related specifically to their job role and industry. Table 18 showcases the participants’ responses. Table 18 showcases no participants indicated more time was spent teaching technical skills compared to technical knowledge that related to their current job role and industry. 6 participants explicitly stated more time was spent teaching technical knowledge. 1 participant’s response was unable to be analyzed due to the wording.

Table 18

Technical Knowledge or Skills Related to Work Role

<table>
<thead>
<tr>
<th>(T.8) Please describe if your institution spent more time teaching cybersecurity technical knowledge or technical skills as it relates specifically to your current job role and industry. Please describe how this time was spent.</th>
</tr>
</thead>
<tbody>
<tr>
<td>“There wasn't really anything specific that they taught related to SOC work besides maybe reading logs, but that was just maybe two class periods, all of the rest of my knowledge has been gotten on my own.”</td>
</tr>
<tr>
<td>“I would say more time was spent teaching knowledge.”</td>
</tr>
<tr>
<td>“The majority of the program was spent teaching technical knowledge. In certain areas within my company it has helped me understand the structure of how certain tasks must be done, and some of how a network functions as a whole. However a lot of the time the program spent</td>
</tr>
</tbody>
</table>
teaching about the knowledge, there was usually no lab or anything that could be used to show us a real life example of how those concepts were executed in a real job.”

“Christian College B spent more time on technical knowledge more than skills.”

“I (?) more time was when on technical knowledge.”

“My institution spent more time teaching cybersecurity technical knowledge relating to my current role. I had a better idea of the why as opposed to the what.”

“More knowledge, but COVID really took away the advantage of the skills.”

Question T.9 requested the participants to discuss any strengths regarding the technical knowledge and skills they developed at their institution as it related to their current job role and industry. Table 19 showcases the participants’ responses. Table 19 showcases 2 participants responded with “not particularly strong”, or “can’t really think of any strengths”. 2 participants responded with “current trends”, or “cybersecurity issues”. Other strengths mentioned are: internships, think like a hacker, general Linux skills, Defense in-depth technologies, and threat recognition.

Table 19

**Technical Strengths Related to Work Role**

(T.9) Please describe any strengths at your cybersecurity program, if any, regarding any technical knowledge and skills you developed as it relates specifically to your current job role and industry.

The technical knowledge was not particularly strong. As mentioned before, the primary strength is in ethical decision making in regards to cybersecurity work.

A strength from my program that relates to my current job was the requirement for two internships before graduation. Through internships not only was I able to learn in the field, but I was able to find the company I currently work for.

Since I am *(a pentester/red team)*, the program really taught me how to think like a hacker.

I did get some general Linux skills, scripting/programming, and understanding of GPOs, and defense in depth items to include firewalls, IDS/IPS, honeypots, DMZ, etc.

A lot of my professors were very knowledgeable and had experience with many issues within cyber security (a lot of them being former/ current military). And the insight and information that they gave to the students based on their experience was invaluable. Some of the security
precautions and organizational skills have helped me out at my job to more easily recognize threats and thus makes more job more secure.

I can't really think of any strengths it was a pretty easy program.

Knowledge was up to date with current trends.

Question T.10 requested the participants to discuss any gaps regarding the technical knowledge and skills they may not have developed at their institution as it related to their current job role and industry. Table 20 showcases the participants’ responses. Table 20 showcases 2 participants responded with “outdated material”. 1 participant indicated no gaps came to mind.

Other gaps mentioned were cloud, hands-on training, data analytics, risk management frameworks, government requirements, and security controls.

Table 20

*Technical Gaps Related to Work Role*

(T.10) Please describe any gaps at your cybersecurity program, if any, regarding any technical knowledge and skills you may not have developed as it relates specifically to your current job role and industry.

“The biggest gap that I wish they had talked more about was getting some information on Cloud. Having a class that only worked on AWS and Azure type stuff would have been a HUGE deal since that could have led people to go into the other highest demand IT field, which is Cloud.”

“Again could have more hands on training.”

“A gap in the program that relates to my current job would be data analytics. Not much time was spent on this topic and being able to review and understand data metrics is very important to my current role.”

“A lot of older protocols and programs were covered.”

“None that I can think of.”

“I certainly had zero clue of RMF and government cyber requirements. I had heard of NIST 800-53, but did not know how security controls worked or were assessed.”

“There was such a broad spectrum of information covered, that some of it may have been outdated. So having a review of the information taught, making sure it relates to the current technology trends would be great."
Question T.11 requested the participants to discuss technical knowledge skills they would ensure would be present if they created their own cybersecurity undergraduate experience that they experienced. Table 21 showcases the responses. The following items were mentioned by 2 participants: “certification preparation”, “red team/ethical hacking”, “networking”, “scripting/programming”, “hardware”, and “attack identification, deterrence, and remediation”.

The following items were mentioned by 1 participant: “policy”, “CTF-style questions”, “vulnerability scanning”, “digital forensics”, “databases”, “firewalls”, “virtual machines”, “up-to-date information”, and “more hands-on training”.

Table 21

**Technical Recommendations Experienced**

<table>
<thead>
<tr>
<th>(T.11) If you were to create a cybersecurity undergraduate experience, what technical knowledge and skills would you ensure were present in your program that you experienced?</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Basic computer hardware Networking Cyber policy Scripting Red Teaming activities”</td>
</tr>
<tr>
<td>“I think any good cybersecurity program should have a strong foundation. So I would ensure to include the basic foundation such as hardware, networking, and a general “What is cybersecurity?” class.”</td>
</tr>
<tr>
<td>“More emphasis on earning certs to go with the knowledge.”</td>
</tr>
<tr>
<td>“A programming course (Java or Python), CTF style challenges, running a vuln scan, digital forensics, what a database is and how it functions, understanding firewalls, how to use a virtual machine.”</td>
</tr>
<tr>
<td>“If I were to create a program, I would ensure that Networking is taught throughout and students have both technical knowledge and skills that would prepare them for the real world. Enough that they would be able to take the CCNA/ Network+ with minimal studying. I would also ensure that students had the knowledge to be able to identify new/existing threats. And have the skills to prevent major damage happen to their future company infrastructure. And understood Information Security well enough to take the Security + exam right out of college.”</td>
</tr>
<tr>
<td>“I would make sure that there would be a lot of information on ethical hacking, and how exactly each major type of attack can be deterred.”</td>
</tr>
<tr>
<td>“I would be sure that information is up to date because trends change. I would develop a program to have more hands-on training even for remote learners.”</td>
</tr>
</tbody>
</table>
Question T.12 requested the participants to discuss technical knowledge skills they would ensure would be present if they created their own cybersecurity undergraduate experience that they did not experience. Table 22 showcases the responses. 3 participants responded with “Blue teaming” or related items (e.g., SIEM, MISP, and threat prevention). The following items were mentioned by 2 participants: “Different OSs (Kali Linux, Linux, Security Onion)”, “cloud/cloud security”, and “terminal/cmd/PowerShell”. The following items were mentioned by 1 participant: “online learning platform (TryHackMe)”, “programming”, “servers”, and “computer system troubleshooting”. 1 participant claimed they couldn’t think of anything to add they did not experience.

Table 22

Technical Recommendations Not Experienced

(T.12) If you were to create a cybersecurity undergraduate experience, what technical knowledge and skills would you ensure were present in your program that you did not experience?

“Linux / Cmd / Powershell skills, PenTesting skills/methodology, SIEM usage, MISP, cloud skills, and different OS such as Kali or Security Onion. Also TryHackMe (soooo many modules exist that teach very well)”

“I would want to put in a cloud and cloud security class, that teaches the basics of AWS and Azure.”

“I would ensure that every student understands how to use the different operating systems, like Kali Linux and Mac OS. And how to use their command lines. I would also ensure that students have a good understanding on how code is structured in the different programming languages.”

“Protection of servers and how to find security threats and how to prevent them.

Blue Team Activities”

“More troubleshooting computer systems.”

“I can’t think of anything I would add that I did not experience.”

Question T.13 requested the participants to discuss anything else related to technical strengths or gaps they experienced at their institution. Table 23 showcases the responses. This is
to allow the participants to freely express anything else that may not have been covered in the
previous questions that should be taken into consideration for Research Question #1. The
following items were mentioned by 1 participant: “incredible professors”, “great experience”,
“hands-on demos and walkthroughs help more than a textbook”, “textbooks are being utilized
that cannot be followed due to being outdated”, and “lack of enforcing cybersecurity
certifications is a gap”.

Table 23

**Additional Technical Strengths and/or Gaps Experienced**

<table>
<thead>
<tr>
<th>(T.13) Is there anything else you would like to share regarding describing, if any, technical skill strengths and/or gaps you experienced at your cybersecurity undergraduate program?</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Not that I can think of, besides the fact that the biggest strength that Christian College A has is that the professors are incredible, and the care that they show is what causes major growth in students.”</td>
</tr>
<tr>
<td>“Hands on demo's and walkthroughs help a lot more than reading from a textbook. Especially when the text book is 2 years old and the steps can no longer be followed.”</td>
</tr>
<tr>
<td>“N/A”</td>
</tr>
<tr>
<td>“No”</td>
</tr>
<tr>
<td>“Nothing about the importance of certs for the job hunt.”</td>
</tr>
<tr>
<td>“None”</td>
</tr>
<tr>
<td>“I sounded negative in my answers but I did have a great experience at college and if I didn't have the information taught to me I would not have been able to be in the position I am right now.”</td>
</tr>
</tbody>
</table>

Research Question #2

As stated previously, the Non-Technical section contained the following 13 questions
directly related to answering Research Question #2 “How would a recent graduate describe, if
any, non-technical skill strengths and gaps commonly experienced in Christian cybersecurity
undergraduate programs?”. The following 13 tables (Table 24 – 36) showcase the responses to
the 13 questions asked in the Technical section of the survey. These questions will be labeled NT.1 through NT.13.

Question NT.1 requested the participant’s satisfaction regarding the non-technical knowledge and skills learned from their institution. Table 24 showcases that 1 participant responded extremely positively with “Very Satisfied”, 5 participants responded with “Yes” or “Satisfied”, and 1 participant responded with “No”.

**Table 24**

**Overall Non-Technical Satisfaction**

<table>
<thead>
<tr>
<th>Technical Satisfaction Level</th>
<th>Number of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Very Satisfied”</td>
<td>1</td>
</tr>
<tr>
<td>“Yes”/“Satisfied”</td>
<td>5</td>
</tr>
<tr>
<td>“No”</td>
<td>1</td>
</tr>
</tbody>
</table>

Question NT.2 requested the participants to go into further detail explaining their satisfaction regarding the non-technical knowledge and skills learned from their institution. Table 25 showcases the participants’ responses. Zoho’s sentiment analysis indicated 4 participants responded with happy sentiment, 1 participant responded with neutral sentiment, 1 participant responded with disappointed sentiment, and 1 participant responded with anger sentiment. Zoho’s sentiment analysis can be found in Figure 8.
Table 25

**Overall Non-Technical Satisfaction Detailed**

(NT.2) Please describe in more detail your satisfaction level with the non-technical knowledge and skills your institution helped you develop.

“I am very satisfied that the school was continually enforcing soft skills and ethics.”
“I feel like it has helped me manage time and learn to teach myself technical skills well.”
“I am satisfied with the non technical knowledge that was provided from my program.”
“I feel like all of that was a waste of time.”
“My institution took time to make sure that the essential information of cybersecurity was taught well and in great detail.”
“I did learn about policies, standards / frameworks, and program management. All very critical.”
“I would have liked to have more knowledge and learning on how to get into the cybersecurity field once graduated.”

**Figure 8**

**Sentiment Analysis of Overall Non-Technical Satisfaction Detailed Responses**

Question NT.3 requested the participants to discuss if their institution spent more time teaching technical knowledge or technical skills. Table 26 showcases the participants’ responses. Table 26 showcases 6 participants indicated more time was spent learning non-technical knowledge. 1 participant indicated more time was spent learning non-technical skills.
**Table 26**

*Non-Technical Knowledge or Skills*

(NT.3) Please describe if your institution spent more time teaching cybersecurity non-technical knowledge or non-technical skills. Please describe how this time was spent.

“Non-technical knowledge for sure”

“More time was spent on non-technical knowledge. I learned what items were part of a cyber program, I did not hand craft each one.”

“I would say more time was spent on the non-technical knowledge. Christian College A saw it very important to form us with good morals and ethics alongside the technical knowledge.”

“More skills”

“I would say that it taught non-technical knowledge, as there is a lot to cybersecurity and it is nearly impossible to cover each item in gruesome detail.”

“More time was spent on knowledge.”

“Non technical knowledge was definitely learned more often. This meant a lot of book knowledge, and basic concepts, rather than getting really granular with specific software or ideas.”

Question NT.4 requested the participants to discuss any strengths regarding the non-technical knowledge and skills they developed at their institution. Table 27 showcases the participants’ responses. Table 27 showcases 2 participants indicated “ethics/morals” and “professors’ knowledge”. Table 27 showcases 1 participant indicated “soft skills”, “resourcefulness”, “compliance frameworks and standards”, and “incident response and contingency policy/planning”. 1 participant indicated no strengths came to mind.

**Table 27**

*Non-Technical Strengths*

(NT.4) Please describe any strengths at your cybersecurity program, if any, regarding the non-technical knowledge and skills your institution helped you develop.

“Their strengths stem from ethics and soft skills.”

“It taught us to be resourceful with our work and issues we have”
“A strength of the program was its formation of us as a good person and not just good at the job. Morals, ethics, and Christian were very involved in the program.”

“Professors knowledge.”

“Having professors that knew the jobs and had experience within them, really helped translate the information taught in the textbooks to the class room and helped students have a deeper understanding of the information taught.”

“I learned about compliance frameworks and standards, and even had to write an IR and contingency policy-plan.”

“None I can think of”

Question NT.5 requested the participants to discuss any gaps regarding the non-technical knowledge and skills they developed at their institution. Table 28 showcases 3 participants indicated no gaps. 2 participants indicated “networking”; however, this researcher believes networking does not fit the non-technical description and rather fits the technical description.

The following items were mentioned by 1 participant: “frameworks”, “assessments”, “security controls”, “lack of preparation for the workforce”, and “hardening”.

**Table 28**

*Non-Technical Gaps*

(NT.5) Please describe any gaps at your cybersecurity program, if any, regarding any non-technical knowledge and skills you may not have developed.

“I cannot think of any gaps in the non-technical knowledge.”

“I did not understand how frameworks guided compliance. No clue how assessments worked, what security controls were, etc.”

“No gaps.”

“As previously stated I wish that my program taught more into the Networking knowledge. We had one or two classes centered around it, when there is so much more that goes into it than that in cybersecurity.”

“Can't think of any”

“Not enough time spent on getting students prepared for the working world.”

“We were not taught many things like simple concepts of networking and system hardening twice, which led to knowledge erosion over the course of my college career.”
Question NT.6 requested the participants to discuss their satisfaction regarding the non-technical knowledge and skills they developed at their institution as it relates to their current job role and industry. Table 29 showcases the participants’ responses. Table 29 showcases 5 participants responded positively with “Yes” or “Satisfied”, 1 participant responded with “Somewhat Satisfied”, and 1 participant responded with “No”.

Table 29

*Non-Technical Satisfaction Related to Work Role*

<table>
<thead>
<tr>
<th>(NT.6) Are you satisfied with the non-technical knowledge and skills your institution helped you develop as it relates specifically to your current job role and industry?</th>
<th>Number of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Yes”/“Satisfied”</td>
<td>5</td>
</tr>
<tr>
<td>“Somewhat Satisfied”</td>
<td>1</td>
</tr>
<tr>
<td>“No”</td>
<td>1</td>
</tr>
</tbody>
</table>

Question NT.7 requested the participants to go into further detail explaining their satisfaction regarding the non-technical knowledge and skills they developed at their institution as it relates to their current job role and industry. Table 30 showcases the participants’ responses. 5 participants responded with various supporting reasons why they were satisfied. These items included: “ethics/morals”, “SSO/MFA”, “policy and system securing planning”, and “adaptability to teach myself new hardware and software basics”. “Ethics/morals” was the only item responded by 2 participants. 1 participant indicated no help was given to look for a job in cybersecurity. 1 participant indicated no non-technical skills or knowledge learned in their institution relates to their job.
Table 30

**Non-Technical Satisfaction Related to Work Role Detailed**

(NT.7) Please describe in more detail your satisfaction level with the non-technical knowledge and skills your institution helped you develop as it relates specifically to your current job role and industry.

“The non-technical knowledge helped with my current job because I was able to go into the workspace with the understanding of what makes cybersecurity so important and the morals of wanting to do good.”

“As stated I work in Identity Access Management, and that relates to many things like SSO/MFA. And having a deep understanding of both of those processes has really helped get my career moving along.”

“I did have to write a policy and a system security plan. Looking back these are not very quality now, but they were a good start into documentation.”

“It has made me versatile, and I have learned to quickly teach myself the basics of new software and hardware pretty easily, which comes from that adaptability.”

“No time was spent getting me prepared to look for a job in cybersecurity.”

“Since I am on the red team side, the ethics class that I took really helps me stay honest.”

“Nothing relates to my job I can think of.”

Question NT.8 requested the participants to discuss if their institution spent more time teaching non-technical knowledge or non-technical skills as it related specifically to their job role and industry. Table 31 showcases the participants’ responses. Table 31 showcases 5 participants indicated more time was spent teaching non-technical knowledge compared to non-technical skills that related to their current job role and industry. Table 31 also showcases 2 participants indicated more time was spent teaching non-technical skills compared to non-technical knowledge that related to their current job role and industry.
Table 31

Non-Technical Knowledge or Skills Related to Work Role

(NT.8) Please describe if your institution spent more time teaching cybersecurity non-technical knowledge or non-technical skills as it relates specifically to your current job role and industry. Please describe how this time was spent.

“More time was spent non-technical knowledge”

“More was spent on knowledge. Since I was a remote learner, more time was spent learning through the textbooks require for the class.”

“It definitely spent more time on the Non-technical knowledge. There are many jobs within InfoSec, so it is impossible to cover all the skills needed for each job in 4 years time. But the concepts taught in each class can better prepare students for whatever job they may receive.”

“More skills.”

“More time was given to knowledge. I had an entire program management and system life cycle class teach how to complete projects and what was needed for successful projects.”

“Non-technical skills”

“It was based on knowledge. More like book information and legal stuff a lot of the time even.”

Question NT.9 requested the participants to discuss any strengths regarding the technical knowledge and skills they developed at their institution as it related to their current job role and industry. Table 32 showcases the participants’ responses. Table 32 showcases 3 participants responded with “no strengths”. Table 32 showcases 2 participants responded with “ethics/morals”. 1 participant responded with “policies” and “frameworks” while another participant indicated “authentication” and “encryption”.

Table 32

Non-Technical Strengths Related to Work Role

(NT.9) Please describe any strengths at your cybersecurity program, if any, regarding any non-technical knowledge and skills you developed as it relates specifically to your current job role and industry.

“The strengths in non-technical knowledge was the morals, faith, and ethics which formed me to go into my job wanted to do good and make a difference.”
“Writing policies and knowing frameworks and standards is important. Understand NIST and ISO.”

“There really are no stand out strengths”

“Having an understanding of the different methods of authentications and encryption keys really helped me out in my job, and if I went into my job without understanding those subjects I would have been in deep water.”

“None”

“Can't think of any”

“Ethics from a Bible perspective. Soft skills.”

Question NT.10 requested the participants to discuss any gaps regarding the non-technical knowledge and skills they may not have developed at their institution as it related to their current job role and industry. Table 33 showcases the participants’ responses. Table 33 showcases 5 participants indicated no gaps. 1 participant indicated “policies”, “security controls”, and “compliance”, while another participant indicated “teaching yourself on the job”.

Table 33

Non-Technical Gaps Related to Work Role

(NT.10) Please describe any gaps at your cybersecurity program, if any, regarding any non-technical knowledge and skills you may not have developed as it relates specifically to your current job role and industry.

“None.”

“I did not realize why policies were important, that nearly anyone can be in charge of documentation, and what security controls were and how they are used to measure compliance.”

“can't think of any”

“There are non that I can think of specifically, since each company structures their information differently. So maybe a deeper understanding of data/network structure would have been nice.”

“I cannot think if any gaps”

“None”

“The primary weakness is that it is not addressed often how much you will need to go and teach yourself a skill when you are on the job, no matter the field.”
Question NT.11 requested the participants to discuss non-technical knowledge skills they would ensure would be present if they created their own cybersecurity undergraduate experience that they experienced. Table 34 showcases the responses. “Ethics/morals” was mentioned by 2 participants. The following items were mentioned by 1 participant: “network operations”, “data structure”, “disaster recovery”, “project management professional (certification)”, “(outside of school) life preparation”, “policy writing”, “incident response plan”, “laws”, “standards”, “frameworks”, “API guides”, and “self-learning software”.

Table 34

Non-Technical Recommendations Experienced

<table>
<thead>
<tr>
<th>(NT.11) If you were to create a cybersecurity undergraduate experience, what non-technical knowledge and skills would you ensure were present in your program that you experienced?</th>
</tr>
</thead>
<tbody>
<tr>
<td>“I would ensure that my students had a deep understanding on network operations and all that encompasses that. I would also ensure that students understand how information is structured and kept.”</td>
</tr>
<tr>
<td>“Disaster recovery and PMP”</td>
</tr>
<tr>
<td>“I would like to have a program that prepared a student for life outside of school. What to expect once you are in the working world would be very helpful.”</td>
</tr>
<tr>
<td>“Ethics from a Bible perspective. Soft skills.”</td>
</tr>
<tr>
<td>“Write a policy, create an incident response plan, know what laws, standards, frameworks exist and to who they apply.”</td>
</tr>
<tr>
<td>“I would ensure that the same morals, ethics, and faith would be present that I experienced.”</td>
</tr>
<tr>
<td>“I would want to make sure that they know how to efficiently search API guides and things like that to teach themselves software”</td>
</tr>
</tbody>
</table>

Question NT.12 requested the participants to discuss non-technical knowledge skills they would ensure would be present if they created their own cybersecurity undergraduate experience that they did not experience. Table 35 showcases the responses. 3 participants responded with “none”. The following items were mentioned by 1 participant: “extra credit for self-learning”,
“assessments”, “risk management frameworks”, “incident response”, “current/up-to-date information”, and “(outside of school) life preparation”.

Table 35

Non-Technical Recommendations Not Experienced

<table>
<thead>
<tr>
<th>(NT.12) If you were to create a cybersecurity undergraduate experience, what non-technical knowledge and skills would you ensure were present in your program that you did not experience?</th>
</tr>
</thead>
<tbody>
<tr>
<td>“I cannot think of anything I would add that I did not experience”</td>
</tr>
<tr>
<td>“I would want to give students the option of extra credit if they do something without any additional instruction, by teaching themselves.”</td>
</tr>
<tr>
<td>“More DR”</td>
</tr>
<tr>
<td>“Explain cyber assessments, define how RMF works, incident response procedures”</td>
</tr>
<tr>
<td>“I can't think of any, I would just make sure that the information taught is current and that students aren't left wanting more out of each lesson.”</td>
</tr>
<tr>
<td>“None.”</td>
</tr>
<tr>
<td>“Above (I would like to have a program that prepared a student for life outside of school. What to expect once you are in the working world would be very helpful.)”</td>
</tr>
</tbody>
</table>

Question NT.13 requested the participants to discuss anything else related to non-technical strengths or gaps they experienced at their institution. This is to allow the participants to freely express anything else that may not have been covered in the previous questions that should be taken into consideration for Research Question #2. Table 36 showcases 5 participants responded with “no/none”. The following items were mentioned by 1 participant: “policies”, “ethics”, and “Bible classes”.

Table 36

**Additional Non-Technical Strengths and/or Gaps Experienced**

(NT.13) Is there anything else you would like to share regarding describing, if any, non-technical skill *strengths* and/or *gaps* you *experienced* at your cybersecurity undergraduate program?

“In college I thought policies were dumb and I'd never write one unless I was in leadership, I was wrong. Show the importance of these items.”

“None”
“None”
“No”
“Ethics and the Bible classes are vital to any cyber program.”
“Not that I can think of.”
“No”

Research Question #3

As stated previously, the Whole-Person section contained the following 13 questions directly related to answering Research Question #3 “How would a recent graduate describe, if any, whole-person skill strengths and gaps commonly experienced in Christian cybersecurity undergraduate programs?” The following 14 tables (Table 37 – 50) showcase the responses to the 14 questions asked in the Whole-Person section of the survey. These questions will be labeled WP.1 through WP.14.

Question WP.1 requested the participant’s satisfaction regarding the whole-person development learned from their institution. Table 37 showcases the responses. Table 37 showcases 5 participants responded positively with “Yes” or “Satisfied”. 1 participant responded with “It was ok”. 1 participant responded with “Not really because of the school specifically”.


**Table 37**

**Overall Whole-Person Satisfaction**

(WP.1) Are you satisfied with the whole-person development your institution helped instill within you? Whole-person may include personal, spiritual, or other non-cybersecurity development.

<table>
<thead>
<tr>
<th>Technical Satisfaction Level</th>
<th>Number of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Yes”/“Satisfied”</td>
<td>5</td>
</tr>
<tr>
<td>“It was ok”</td>
<td>1</td>
</tr>
<tr>
<td>“Not really because of the school specifically”</td>
<td>1</td>
</tr>
</tbody>
</table>

Question WP.2 requested the participants to go into further detail explaining their satisfaction regarding the whole-person development learned from their institution. Table 38 showcases the participants’ responses. Zoho’s sentiment analysis indicated 4 participants responded with happy sentiment, 2 participants responded with disappointed sentiment, and 1 participant responded with neutral sentiment. Zoho’s sentiment analysis can be found in Figure 9.

**Table 38**

**Overall Whole-Person Satisfaction Detailed**

(WP.2) Please describe in more detail your satisfaction level with the whole-person development your institution helped instill within you.

““It was ok. I think the whole-person concept is overrated but I was going back after service in the (military) so I just saw it a waste of time.”

“Very satisfied. Morals, faith, and ethics played a large part in the curriculum to prepare us to be good people and not just good professionals.”

“I was able to be involved in and lead efforts in Campus Ministries, the Cyber club, and Intramural sports. This variety of activities developed me into a strong, well-rounded individual.”

“I was very satisfied with what the professors could do by incorporating the Christian message into their lessons on Cybersecurity topics, which is difficult to do with such a technical program. And the communication/interpersonal skills I personally grew in were invaluable.”
“I was satisfied with the whole person education. Christian College B spent time with courses that developed you as a Christian leader.”

"There was a slight push to grow not only as a student, but also as a healthy Christian, but this push came from my RD and professors and was not because of school policy or anything.

“The cyber program at my school really molded me into personable engineer.”

Figure 9

_Sentiment Analysis of Overall Whole-Person Satisfaction Detailed Responses_

![Sentiment Analysis](image)

Question WP.3 requested the participants to discuss how their institution spent time with whole-person development. Table 39 showcases the participants’ responses. Table 39 showcases 4 participants responded with “connecting/community/friendship/interaction” with “cyber majors, other undergraduates, residence directory, or faculty”. Table 39 showcases 2 participants responded with “Biblical classes”.

Table 39

_Whole-Person Development Time_

<table>
<thead>
<tr>
<th>(WP.3) Please describe how your institution spent time with your whole-person development.</th>
</tr>
</thead>
<tbody>
<tr>
<td>“I spent the majority of my time with other cyber majors and still continue to connect with them and grow.”</td>
</tr>
<tr>
<td>“About half the time (?)”</td>
</tr>
<tr>
<td>“Biblical and leadership classes.”</td>
</tr>
<tr>
<td>“Morals, faith, and ethics played a large part in the curriculum to prepare us to be good people and not just good professionals.”</td>
</tr>
<tr>
<td>“My School had classes focused entirely around Doctrine and Theology, which were great for growing in my faith. In my classes we also had discussion boards were we would interact with fellow students and discuss that weeks information.”</td>
</tr>
</tbody>
</table>
“The institution didn't do anything, but my professors and RD spent a lot of time speaking with me about things like spiritual development, but this is because I had a personal friendship with them.”

“Christian College B was big on spiritual development. It was easy to find community and those with the same goals as you if you sought it out. We had small groups on each hall that helped grow community and strengthen spiritual lives, and a weekly chapel service (specific details redacted).”

Question WP.4 requested the participants to discuss any strengths regarding the whole-person development learned from their institution. Table 40 showcases the participants’ responses. Table 40 showcases “leadership development” was mentioned by 2 participants. The following items were mentioned by 1 participant: “morals/faith/ethics”, “communication skills”, “servant’s heart”, and “community growth”. 1 participant indicated “none”, while another participant indicated “staff (not institution) helped whole-person development”.

Table 40

**Whole-Person Strengths**

(WP.4) Please describe any strengths, if any, regarding the whole-person development your institution helped instill within you.

“Morals, faith, and ethics played a large part in the curriculum to prepare us to be good people and not just good professionals.”

“With a lot of the classes I took being online I had to email my professors frequently and that helped me develop communication skills that let me express my questions and frustrations in a respectful manner.”

“Christian College B developed me as a leader. Classes on leadership were extremely helpful to develop me as a person.”

“Having been able to serve in positions of leadership, I gained a servant's heart and saw the impact one can make on others. I had people pouring into me, and that allowed me to pour into others.”

“The institution really emphasized community growing.”

“None”

“The institution did not do anything. It was all the staff, not because of anything the school in a whole sponsored”
Question WP.5 requested the participants to discuss any gaps regarding the whole-person development learned from their institution. Table 41 showcases the participants’ responses.

Table 41 showcases 5 participants responded with “no gaps”. 1 participant responded with “occasional ostracizing non-Christians/lack of loving people”. 1 participant responded with “disconnect between directors and students”, “interested in dishing out consequences”, “lack of grace”, and “not touch a heart”.

**Table 41**

**Whole-Person Gaps**

(WP.5) Please describe any gaps at your institution, if any, regarding any whole-person development that may not have been instilled within you.

<table>
<thead>
<tr>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>“None”</td>
</tr>
<tr>
<td>“I cannot think of any.”</td>
</tr>
<tr>
<td>“None.”</td>
</tr>
<tr>
<td>“Occasional ostracizing on campus of those that were not Christian. It was not difficult to see who did not fit in. A better job of loving these people could have been stressed.”</td>
</tr>
<tr>
<td>“The primary gap is the disconnect between higher tier directors and the student population. They seemed to be too interested in dishing out consequences, when they really had the option to show grace in that moment and have a good chance to touch a heart.”</td>
</tr>
<tr>
<td>“No gaps”</td>
</tr>
<tr>
<td>“None.”</td>
</tr>
</tbody>
</table>

Question WP.6 requested the participants to discuss their satisfaction regarding the whole-person development learned from their institution as it relates to their current job role and industry. Table 42 showcases the participants’ responses. Table 42 showcases 4 participants responded positively with “Yes” or “Satisfied”, 2 participants responded negatively with “No”, and 1 participant responded with “I can’t see a correlation”.
Table 42

**Whole-Person Satisfaction Related to Work Role**

(WP.6) Are you satisfied with the whole-person development your institution helped instill within you as it relates specifically to your current job role and industry?

<table>
<thead>
<tr>
<th>Technical Satisfaction Level</th>
<th>Number of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Yes”/“Satisfied”</td>
<td>4</td>
</tr>
<tr>
<td>“No”</td>
<td>2</td>
</tr>
<tr>
<td>“I can’t see a correlation”</td>
<td>1</td>
</tr>
</tbody>
</table>

Question WP.7 requested the participants to go into further detail explaining their satisfaction regarding the whole-person development learned from their institution as it relates to their current job role and industry. Table 43 showcases the participants’ responses. Table 43 showcases 3 participants responded with “same as before (no development)”, “nothing relating to it”, or “N/A”. The following items were mentioned by 1 participant: “Christian leadership development”, “morals/faith/ethics”, “involvement across campus”, “interpersonal skills”, and “communication skills”.

Table 43

**Whole-Person Satisfaction Related to Work Role Detailed**

(WP.7) Please describe in more detail your satisfaction level with the whole-person development your institution helped instill within you as it relates specifically to your current job role and industry.

“Developing a person as a Christian leader and given them that foundation really helps a person to adapt and handle any work situation that is thrown at them.”

“Morals, faith, and ethics played a large part in the curriculum to prepare us to be good people and not just good professionals.”

“It is the same as before.”
“I was able to be involved in Campus ministries, intramural sports, and cyber, all 3 vastly different. Being with differing groups of people has helped me to relate and interact with those I know consult.”

“All the interpersonal skills I learned in college, I am able to effectively communicate with my coworkers and get work done in an efficient manor.”

“Nothing relating to it”

“N/A”

Question WP.8 requested the participants to explain how the institution spent time regarding developing the participant from a whole-person perspective as it relates to their current job role and industry. Table 44 showcases the participants’ responses. Table 44 showcases 3 participants responded with “none” or “no relation/correlation”. 2 participants mentioned “faith strengthening”, “foundation”, and “Christian leadership development”. The following items were mentioned by 1 participant: “online communication”, “morals/ethics”, “speaking confidently”, and “management”.

Table 44

Whole-Person Development Time Related to Work Role

Please describe how your institution spent time with your whole-person development as it relates specifically to your current job role and industry.

“The need to discuss online with my fellow students really helped build a good foundation on how to communicate online (as I work from home). It also helped build me in my Faith so that I am able to stand up for what I believe and be firm in my faith.”

“Morals, faith, and ethics played a large part in the curriculum to prepare us to be good people and not just good professionals.”

“Developing a person as a Christian leader and given them that foundation really helps a person to adapt and handle any work situation that is thrown at them.”

“None”

“I was placed in positions of leadership in college and this prepared me to speak confidently, lead with actions, and manage others effectively in my current role.”

“There isn't a correlation that I can make.”

“I feel like it doesn't really relate right now.”
Question WP.9 requested the participants to discuss any strengths regarding developing the participant from a whole-person perspective as it relates to their current job role and industry. Table 45 showcases the participants’ responses. Table 45 showcases 3 participants responded with “none”, “no relation”, or “N/A”. 2 participants responded with “faith”. The following items were mentioned by 1 participant: “ethics/morals”, “leadership and Bible classes”, “desire for excellence”, “heart to help”, “discussions inside and outside the classroom”.

**Table 45**

**Whole-Person Strengths Related to Work Role**

<table>
<thead>
<tr>
<th>(WP.9) Please describe any strengths, if any, regarding your whole-person development your institution helped instill within you as it relates specifically to your current job role and industry.</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Morals, faith, and ethics played a large part in the curriculum to prepare us to be good people and not just good professionals.”</td>
</tr>
<tr>
<td>“Leadership classes and Bible classes instilled a strong Christian foundation.”</td>
</tr>
<tr>
<td>“N/A”</td>
</tr>
<tr>
<td>“I feel like it doesn't really relate right now.”</td>
</tr>
<tr>
<td>“None”</td>
</tr>
<tr>
<td>“I gained a desire for excellence, and a heart to help others through service projects. It helped build my confidence in my faith, by having discussion about theology and doctrine not only in class but outside of it as well.”</td>
</tr>
</tbody>
</table>

Question WP.10 requested the participants to discuss any gaps regarding developing the participant from a whole-person perspective as it relates to their current job role and industry. Table 46 showcases the participants’ responses. Table 46 showcases 6 participants responded with either “none” or “N/A”. The following items were mentioned by 1 participant: “group projects”, and “lack of learning how to work together effectively”.

Table 46

Whole-Person Gaps Related to Work Role

(WP.10) Please describe any gaps at your institution, if any, regarding any whole-person development that may not have been instilled within you as it relates specifically to your current job role and industry.

“Group projects tend to leave me with distrust for others, as the over-achiever I am. Working together is a must in a career, it would help to learn to do this effectively in college.”

“None”

“None”

“None that I can think of.”

“I feel like it doesn't really relate right now.”

“N/A”

“No gaps”

Question WP.11 requested the participants to discuss whole-person development they would ensure would be present if they created their own cybersecurity undergraduate experience that they experienced. Table 47 showcases the responses. 2 participants responded with “ethics/morals”. The following items were mentioned by 1 participant: “leadership classes”, “Bible history classes”, “theory classes”, “faith”, “Word of God”, and “community”. 1 participant responded they wanted “less whole-person development”.

Table 47

Whole-Person Recommendations Experienced

(WP.11) If you were to create a cybersecurity undergraduate experience, what whole-person development would you ensure were present in your program that you experienced?

“I would just ensure that there were ethics courses.”

“Same leadership and Bible history and theory classes.”

“I would make sure to integrate the same foundation of good morals, ethics, and faith that I experienced.”

“N/A”
“Less of it”
“I would ensure that the word of God is incorporated into every class, even if it doesn’t relate to the content of that day’s class, that discussion is much needed.”
“A focus on community, all college age people strongly desire this, even computer majors.”

Question WP.12 requested the participants to discuss whole-person development they would ensure would be present if they created their own cybersecurity undergraduate experience that they did not experience. Table 48 showcases the responses. 3 participants responded with “none” or “N/A”. The following items were mentioned by 1 participant: “opportunities for women in cyber”, “free certifications”, “more grace”, “more interpersonal skills”, and “ensure students are confident in interviews”. 1 participant responded they wanted “less whole-person development”.

Table 48

**Whole-Person Recommendations Not Experienced**

<table>
<thead>
<tr>
<th>(WP.12) If you were to create a cybersecurity undergraduate experience, what whole-person development would you ensure were present in your program that you did not experience?</th>
</tr>
</thead>
<tbody>
<tr>
<td>“N/A”</td>
</tr>
<tr>
<td>“Creating space for women in cyber, it's often a male dominated field. Also offer Security+ for free. Students should come out with a degree and cert.”</td>
</tr>
<tr>
<td>“Less of the whole concept.”</td>
</tr>
<tr>
<td>“Cannot think of something I did not experience”</td>
</tr>
<tr>
<td>“None”</td>
</tr>
<tr>
<td>“I would have liked to have seen a little bit more grace shown to some of my colleagues, rather than being so quick to the whip.”</td>
</tr>
<tr>
<td>“I would include more interpersonal skill development. Because some of the kids are quiet and can come off as unconfident in interviews for future jobs.”</td>
</tr>
</tbody>
</table>

Question WP.13 requested the participants to discuss Biblical whole-person development strengths or weaknesses they encountered at their institution. Table 49 showcases the responses.
4 participants responded with various strengths (e.g., faithfulness, steadfastness, love, compassion, strength, stand strong in faith). 2 participants responded with “Not really” or “Not necessarily”. 1 participant responded “college lacks in nearly all of those Biblical whole-person traits”.

**Table 49**

*Whole-Person Biblical Traits Strengths or Weaknesses*

<table>
<thead>
<tr>
<th>(WP.13) Using Philippians 4:8, Matthew 5:8, 1 Timothy 4:12, and 1 Corinthians 16:13-14 as references, did you specifically experience any strengths or weaknesses at your institution with these Biblical whole-person traits: speech, conduct, love, faith, purity, strength, steadfastness, faithfulness, and/or being on guard? Feel free to elaborate on other Biblical whole-person traits you may or may not have experienced</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Not really”</td>
</tr>
<tr>
<td>“I got to lead a small group one year, lots of faithfulness, steadfastness, and love were experienced through this. For maybe the first time I felt proud of others when they experienced success or breakthrough.”</td>
</tr>
<tr>
<td>“I feel as if Christian College A lacks in nearly all of those. They tried to add on charges to my bill every semester, tried to tell me over and over that that was the real bill until I went over their head, then it got sorted. People got in trouble for things that weren't really necessary, while some athletes got grace just because they are national class athletes. There were many times that some people got major penalties while others got turned a blind eye and it is unethical and wrong completely from a christian point of view.”</td>
</tr>
<tr>
<td>“Christian College B spent the undergraduate program focused on the whole person biblical traits. The University showed love and compassion for their students. The classes helped instill strength, steadfastness and faithfulness. After graduating I did feel that my education from Christian College B gave me a strong Christian foundation that I could take in the real world.”</td>
</tr>
<tr>
<td>“My university made sure that these values were instilled into every student. And that gave not only me but many other students to go out into the secular world and stand strong in our faith.”</td>
</tr>
<tr>
<td>“Yes I experienced the formation of these traits from all involved with the program”</td>
</tr>
<tr>
<td>“Not necessarily since the a lot of the student population where not sincere Christians.”</td>
</tr>
</tbody>
</table>

Question WP.14 requested the participants to discuss anything else related to strengths or gaps regarding whole-person development they experienced at their institution. This is to allow the participants to freely express anything else that may not have been covered in the previous
questions that should be taken into consideration for Research Question #3. Table 50 showcases the responses. 4 participants responded with “No” or “None”. 1 participant responded positively with “faculty opening with word of prayer” and “Biblical passage discussion”. 2 participants responded in a negative manner. 1 participant responded negatively with “Relating cyber to Bible/Jesus makes no sense” and “everyone uses openbible.com and mashes verses that are taken out of context”. This participant also challenges faculty to “find a better way to relate cyber to Christian life”. 1 participant responded negatively by stating “good role models are few and not running the college”.

Table 50

Additional Whole-Person Strengths and/or Gaps Experienced

(WP.14) Is there anything else you would like to share regarding describing, if any, whole-person skill strengths and/or gaps you experienced at your cybersecurity undergraduate program?

“None”

“I felt as though sometimes it were hard to incorporate Christian doctrine into the course work. Especially when you're dealing with something as technical as cyber security. But what some of my professors did, along with teaching the class, would be to open their classes with a word of prayer and discuss certain passages of the Bible. I felt that sometimes that lead to better discussion on what we believe than you would find in a course centered around The Bible.”

“There are good role models at Christian College A, but very few of them are the ones actually running the college. This shouldn't be true. The top level directors and deans should all be of the highest conduct and have the biggest hearts.”

“No”

“No.”

“Relating a network diagram or firewall to the Bible/Jesus makes no sense. Everyone just uses openbible.com and mashes a verse in that really has nothing to do with a topic. This leads to out of context scripture and students that would rather just fake it then put thought into responses. Find a better way to relate cyber to the christian life.”

“No”
Research Question #4

The following table (Table 51) showcases the responses to the 1 question asked in the Cumulative section of the survey. This question will be labeled C.1. Zoho’s sentiment analysis indicated 4 participants responded with happy sentiment, 2 participants responded with disappointment sentiment, and 1 participant responded with anger sentiment. Zoho’s sentiment analysis can be found in Figure 10. Table 51 showcases 3 participants responded with the lack of hands-on material within their Christian cybersecurity program experience. 3 participants noted their program was not very “technical”; however, 2 of the 3 did not see that as a negative. 2 participants mentioned they appreciated the “whole person” development they experienced at their institution. 1 participant stated each class was stand-alone. 1 participant responded how the program should help students better prepare for the workforce. 2 participants responded with the feeling the institution either “lied” or was “shameful” with their business practices. 3 participants responded in a manner that showed appreciation for their faculty/staff. It was challenging to identify themes within this data as a large amount of the data collected did not accurately reflect the initial intent of this research question; however, the overall theme that was identified is that each participant’s experience prior to, during, and after their undergraduate experience and satisfaction are all unique (even at the same Christian program and similar role in the workforce).
Table 51

**Cumulative Undergraduate Experience Essay**

(C.1) Finally, how would you describe your cumulative (increasing by successive additions) experience during your cybersecurity undergraduate experience? Please describe with a 125-250-word essay.

“My time at Christian College B was a great experience. The education that I received was a total whole person experience. My undergraduate studies were spent developing the whole Christian person. Classes on leadership and Biblical history and theory were very influential in helping me develop a strong Christian foundation that has helped me become a stronger Christian and develop me as a better leader. The classes that I took in the Cybersecurity field gave me a foundation that I use in my current field. The professors were very helpful and knowledgeable. I do wish that I would have been able to receive more hands-on training that would have helped me in the current job world. Information technology and Cybersecurity change daily, and Christian College B did a good job keeping up with the changing landscape. I would have liked to have had a program that got the student better prepared to enter the job market and what to expect from the job world. This would be a tremendous help to the upcoming cybersecurity student.”

“While going through my college experience, I first started at a community technical college and eventually transferred to my Christian college in my junior year. I experienced both great and terrible courses, and grew a lot. Not only personally, but in faith. I experienced more hands on experience and felt as though I learned more at my community college, only because the school was centered around giving us students that experience. During my time there I had the opportunity to work with Networking equipment, and understand how firewalls work and how to configure. But when I went to my Christian College I learned the concepts of almost everything that could be covered in cybersecurity. And if I weren’t taught those concepts I wouldn’t be in the position that I am today. I think finding that balance of technical hands-on approach and the technical knowledge of cybersecurity is what institutions should strive for. You can’t have one without the other, and if Christian colleges take this into account we could not only send our future students out with the knowledge to become InfoSec professions, but we could also spread the word of God through our teachings.”

“I believe that most students do not really understand what they are going to learn when they sign up for a cybersecurity degree. They are told big paycheck and easy job, and then become frustrated when it's super hard to land that first role, and it does not come with a 6 figure check. I felt lied to once I had graduated, if not for anything more than I was told how easy it would be to get a job, (which we all know that first job is so difficult to obtain because industry believes you learn nothing from college, which is about 75% true most places). I learned a broad overview of all that cyber encompassed, which I did not mind it. However, others that wanted to be super technical felt they had learned nothing and paid for a degree that didn't get them a job or skills. In the end my desire to self-learn and find resources outside of the classroom is what made the difference. I loved the "whole person" experience, and certainly grew a lot. Cyber changes fast, it's hard to put into curriculum, I get it. Hand's on demos and talks from those currently in the field is some of the most beneficial things you can
offer students. I do think colleges need to be honest with incoming students and not try to sell them something they can not deliver as well.”

“Overall, I am very happy with my cybersecurity ungrad experience. The program is very good with hitting all of the key topics, but not implementing hands-on experience. The best part of the entire degree program is that you are introduced to professionals and competitions that help you in the long run; unfortunately, these opportunities only happen once a year. I really like that I had only 3 cyber professors for the entire program, although it did over work out professors and make certain things happen a little more difficult. To add, this program has already started to implement certain changes into their curriculum, but I wasn't able to partake in the new changes.”

“I am not totally sure what this means by cumulative experience. My college experience was not made good or bad because of my specific degree choice, or college choice. The make or break factor always has been, and always will be the people that I was around. My friends, classmates, professors, and resident director. Those are the people who made college good. As for Christian College A, I have only learned more and more every year that the college is being run like a questionable business, and is out to make money out of whoever they can. That is believable for a normal college, but it is shameful for a Christian college to be seen like that by so many people. The cybersecurity program itself was lackluster, and I had to put in a lot of work myself because either professors were often too lax and just gave everyone good grades because they felt like being nice, or the professor didn't put in the work to make a curriculum and so all of their tests were taken from internet quizzes and they were easily cheated on. This led to a program that was easily passed by anyone, even without creating any real skill in the cybersecurity field. It was really disappointing to see myself studying and working hard, then see someone else just cheating on every test and making higher grades than me in a class that I had really worked hard in.”

“Overall, I was very satisfied with my undergraduate experience at Christian College A. One thing I enjoyed was with Christian College A being a very small school, this meant smaller class sizes which allowed more personal interaction with the classmates and professors. I enjoyed how the program was not specific to technical knowledge. The staff really cared about you being a good person and working to the best of your abilities. Christian College A also holds (cybersecurity events), so it was a bonus as a student being able to experience that each year and listen to so amazing speakers. I would suggest Christian College A to someone looking to purse an education in cybersecurity.”

“Not really I feel like most of the classes were pretty much stand-alone.”
Figure 10

Sentiment Analysis of Cumulative Undergraduate Experience Essay

![Sentiment Analysis Chart]

14.29%  28.57%  57.14%

Evaluation of the Research Design

This study was an online anonymous survey distributed to recent cybersecurity graduates. The primary purpose was to gain a better understanding of the perspectives of recent Christian college and university cybersecurity graduates regarding the holistic experience of their undergraduate academic program as preparation for the workforce. The holistic experience included (technical, non-technical, and whole-person) and attempted to identify any trends regarding strengths and shortcomings (if any). This survey contained a Consent Form page and a Qualification page. Afterwards, the survey contained a section requesting more details about their qualification and four additional sections that addressed technical, non-technical, whole-person and cumulative experiences. The survey overall included 47 questions (Appendix P). The estimated time to complete this survey was 45-minutes. The time to complete from each participant is showcased in Table 52 and Figure 11.

Table 52

Time Taken in Survey (Least to Greatest)

<table>
<thead>
<tr>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>27 mins</td>
</tr>
<tr>
<td>41 mins</td>
</tr>
<tr>
<td>46 mins</td>
</tr>
<tr>
<td>52 mins</td>
</tr>
<tr>
<td>1 hr 47 mins</td>
</tr>
<tr>
<td>2 hrs 6 mins</td>
</tr>
<tr>
<td>2 hrs 18 mins</td>
</tr>
</tbody>
</table>
All surveys were completed online, via Zoho, by the solicited participants that met the requirements for this research. The survey presented 47 open-ended questions that addressed technical, non-technical, whole-person, and cumulative questions regarding the participants' experience at their Christian undergraduate cybersecurity program. Surveys, compared to interviews, focus groups, and observation, were the method with the lowest influence and disruption by the researcher. Surveys are “high level of structure and standardization, commonly used to collect data from large numbers of people, researcher involvement with the participants is low” (Jackson, 2020, p. 125). Due to the researcher bias and/or involvement being high for qualitative research that utilizes interviews, focus groups, or observations, this researcher solely utilized surveys to protect against researcher bias and influence that may taint the perception and quality of this research. This researcher utilized these surveys to distribute, collect, and analyze the satisfaction of cybersecurity graduates of four-year Christian institutions from a technical, non-technical, and whole-person vantage point. This researcher, with experience as a
cybersecurity professional and educator, utilized interviews to gain high trust in the data as to not be tainted by this researcher.

**Chapter Summary**

Chapter Four showcased the study’s findings through collecting and analyzing the survey responses in a qualitative manner. The researcher described the particular steps taken in collecting the data and compiling the data throughout the research methodology and implementation. The researcher then analyzed each of the 47 questions identifying commonalities across technical, non-technical, whole-person, and cumulative responses. Having analyzed this data, Chapter Five will declare conclusions, implications, and applications. The conclusions in Chapter Five are based on the similarities of answers and the sentiment of the responses found in each of the responses of the 7 participants. Afterward, limitations and suggestions for future research will be presented.
CHAPTER FIVE: CONCLUSIONS

Overview
This research was scoped to determine how recent graduates from Christian undergraduate cybersecurity programs felt their academic experience was technically, non-technically, whole-person, and cumulative. Chapter One presented an overview of the study. Chapter Two presented and reviewed relevant literature to inform the study and identify a gap in research related to Christian cybersecurity education. Chapter Three presented the definitions of how the study was completed and the research tools utilized. Chapter Four showcased the study’s findings through collecting and analyzing the survey responses and discovered the specifications of satisfaction for the recent graduates. Having analyzed this data, Chapter Five will now declare conclusions, implications, and applications. The conclusions in Chapter Five are based on the similarities of answers and the sentiment of the responses found in each of the responses of the 7 participants. Afterward, limitations and suggestions for future research will be presented.

Research Purpose
The purpose of this qualitative, exploratory, phenomenological research was to gain an understanding of the perspectives of recent Christian college and university cybersecurity graduates regarding the holistic experience (technical, non-technical, and whole-person) strengths and shortcomings (if any) of their undergraduate academic program as preparation for the workforce. The categories the graduates utilized to describe their holistic undergraduate education were defined as technical, non-technical, and whole-person. The technical category addressed technical cybersecurity topics (e.g., cryptography; networking; network defense; scripting; hacking; etc.). The non-technical category collected data pertinent to their preparation
to perform non-technical cybersecurity topics (e.g., cybersecurity planning and management; policy, legal, ethics, and compliance; security risk analysis; cyber threats; etc.). The whole-person category assessed the non-cybersecurity-related skills and traits they developed at their institution (e.g., love; strength; steadfastness; faithfulness; being on guard; etc.). The gap driving this study was the need to learn how current cybersecurity programs have influenced and molded students for the workforce and allow Christian cybersecurity program leaders to utilize this research and optimize the experience their students have at their institution. The theory guiding this exploratory research was academic outcomes assessment theory in which student opinions were sought to identify the satisfaction relationship their technical, non-technical, and whole-person development in their Christian undergraduate program as preparation for real-world application. The following four research questions as mentioned next guided this study.

**Research Questions**

**RQ1.** How would a recent graduate describe, if any, technical skill strengths and gaps commonly experienced in Christian cybersecurity undergraduate programs?

**RQ2.** How would a recent graduate describe, if any, non-technical skill strengths and gaps commonly experienced in Christian cybersecurity undergraduate programs?

**RQ3.** How would a recent graduate describe, if any, whole-person skill strengths and gaps commonly experienced in Christian cybersecurity undergraduate programs?

**RQ4.** How would a recent graduate describe their cumulative experience at a Christian cybersecurity undergraduate program?

**Research Conclusions, Implications, and Applications**

This study was designed to create a feedback loop that spanned multiple Christian institutions. This research will allow Christian cybersecurity program leaders to self-assess if their programs have any of the strengths or weaknesses, if identified, to allow their own program to continue to improve or change any shortcomings. The data collected gave personal and...
practical information regarding the graduate’s Christian undergraduate cybersecurity experience. Research conclusions, implications, and applications will now be shared. This draws from the analysis and was based on the similarities of answers and the sentiment of the responses that were performed in Chapter Four when examining each of the 7 responses across all 47 open-ended qualitative questions.

Conclusions

Each participant had a unique academic experience regardless of the Christian cybersecurity program. Additionally, each participant identified areas of strengths within their Christian cybersecurity program in at least one of these areas: technical, non-technical, whole-person, and/or cumulative. Furthermore, each participant identified areas of gaps/weaknesses within their Christian cybersecurity program in at least one of these areas: technical, non-technical, whole-person, and/or cumulative. Lastly, this research was delimited to participants that graduates within the last five years; however, the years 2016 through 2018 were unrepresented by participants. Potential participants were identified that graduates within each of these years; however, zero percent of these potential participants partook in the survey during the two weeks it was active. This draws the conclusion that cybersecurity students that have graduated more recently may have been more willing to discuss and elaborate about their academic journey for the betterment of current future Christian cybersecurity student experiences. This conclusion is also supported by Table 7 as only 1 participant completed the survey that graduated in 2019, 2 participants completed the survey that graduated in 2020, and 4 participants completed the survey that graduated in 2021.
Conclusions for Research Question #1

The participants were presented with a request (Question T.1) to share if they are satisfied with the technical knowledge and skills their institution helped them develop. The majority of the participants were not completely satisfied. These answers were “Mildly Satisfied”, “Somewhat Satisfied”, “Not Fully Satisfied”, “Not Really”, and “No”. Only 2 participants selected “Yes” or “Satisfied” when asked about their satisfaction of technical knowledge and skills. According to this research, the participants were least satisfied with their technical development compared to non-technical and whole-person. This is supported by Table 11.

The participants were asked to go into further detail explaining their satisfaction level (Question T.2). 6 participants (out of 7) responded in a manner that described a desire for the institution to provide more technical knowledge and skills or highlighted the institution taught minimal technical knowledge and skills. Only 1 participant responded in a manner that did not describe a desire for the institution to provide more technical knowledge and skills. To further support this, Zoho’s sentiment analysis indicated 3 participants responded with disappointed sentiment, 2 participants responded with neutral sentiment, 1 participant responded with happy sentiment, and 1 participant responded with extremely happy sentiment. This conclusion is supported by Table 12 and Figure 7.

The participants were asked (Question T.4) to discuss any strengths regarding the technical knowledge and skills they developed at their institution. The same percentage of participants claimed that their faculty/staff as a technical strength as claimed their institution had absolutely no technical strengths. Certifications were also a common strength identified by multiple participants. This is supported by Table 14.
The participants were asked (Question T.5) to discuss any gaps regarding the technical knowledge and skills they developed at their institution. The majority of participants directly claimed a gap regarding technical skills (e.g., Linux, cyber operations, penetration testing, threat hunting, SOC, networking, labs were too easy). Only 1 participant claimed there were no technical gaps at their institution. This is supported by Table 15.

The participants were presented with a request (Question T.6) to share if they are satisfied with the technical knowledge and skills their institution helped them develop as it relates to their current job role. Participants were just as likely to state they are not satisfied with the technical knowledge and skills that relate to their current job role compared to stating they are satisfied with the technical knowledge and skills that relate to their current job role. The participants, even though they are hired in a job role, are not satisfied with the institution's ability to develop them technically, not for the entire cybersecurity profession, but just specifically for their single current role. They have been hired; however, do not believe they have been prepared by the institution. This is supported by Table 16.

Each of the participants (who submitted a legible response) explicitly stated more time was spent teaching technical knowledge versus technical skills (Question T.8). This is supported by Table 18.

The participants were asked (Question T.9) to discuss any strengths regarding the technical knowledge and skills they developed at their institution as it related to their current job role and industry. 2 participants responded with “not particularly strong”, or “can’t really think of any strengths”. 2 participants responded with “current trends”, or “cybersecurity issues”. This is supported by Table 19.
The participants were asked (Question T.10) to discuss any gaps regarding the technical knowledge and skills they developed at their institution as it related to their current job role and industry. 2 participants responded with “outdated material”. This is supported by Table 20.

The participants were asked (Question T.11) to discuss technical knowledge skills they would ensure would be present if they created their own cybersecurity undergraduate experience that they experienced. These categories were identified by multiple participants: “certification preparation”, “red team/ethical hacking”, “networking”, “scripting/programming”, “hardware”, and “attack identification, deterrence, and remediation”. These are the key areas that are currently in certain cybersecurity curricula that are appreciated by graduates. This is supported by Table 21.

The participants were asked (Question T.12) to discuss technical knowledge skills they would ensure would be present if they created their own cybersecurity undergraduate experience that they did not experience. 3 participants responded with “Blue teaming” or related items (e.g., SIEM, MISP, and threat prevention). The following items were mentioned by 2 participants: “Different OSs (Kali Linux, Linux, Security Onion)”. These are the key areas that should be considered in all cybersecurity curricula. This is supported by Table 22.

Overall, the purpose of this research question was to identify how a recent graduate would describe, if any, technical skill strengths and gaps commonly experienced in Christian cybersecurity undergraduate programs. Based on this research there is an overwhelming trend of recent cybersecurity graduates that are not fully satisfied with their technical development. This research supports that the overall technical development of undergraduate students preparing for the workforce is the largest gap addressed within this survey.
**Conclusions for Research Question #2**

The participants were presented with a request (Question NT.1) to share if they are satisfied with the non-technical knowledge and skills their institution helped them develop. 6 participants responded in a positive manner (e.g., “Very Satisfied”, “Yes”, or “Satisfied”). According to this research, the participants were most satisfied with their non-technical development compared to technical and whole-person. This is supported by Table 24.

The participants were asked to go into further details explaining their satisfaction level (Question NT.2). 5 participants (out of 7) responded in a manner that did not describe a desire for the institution to provide more non-technical knowledge and skills. 1 participant responded in a manner that requested more knowledge about getting into the workforce, while another participant stated it was “all a waste of time”. To further support this, Zoho’s sentiment analysis indicated 4 participants responded with happy sentiment, 1 participant responded with neutral sentiment, 1 participant responded with disappointed sentiment, and 1 participant responded with anger sentiment. This conclusion is supported by Table 25 and Figure 8.

The participants were asked (Question NT.4) to discuss any strengths regarding the non-technical knowledge and skills they developed at their institution. “Ethics/morals” and “professors’ knowledge” were indicated by 2 participants each. This is supported by Table 27.

The participants were asked (Question NT.5) to discuss any gaps regarding the non-technical knowledge and skills they developed at their institution. The majority of participants directly claimed there is no gap regarding non-technical skills. This is supported by Table 28.

The participants were presented with a request (Question NT.6) to share if they are satisfied with the non-technical knowledge and skills their institution helped them develop as it relates to their current job role and industry. The applicability of being related to their current job
role and industry did not alter the participants’ satisfaction. 6 participants responded in a positive manner (e.g., “Very Satisfied”, “Yes”, or “Satisfied”). This is supported by Table 29.

The majority of participants were unable to identify any gaps regarding the non-technical knowledge and skills they developed at their institution as it related to their current job role and industry. This is supported by Table 33.

Besides “ethics/morals” there was not a non-technical skill that was identified by multiple participants that they would want present within a cybersecurity program. This is supported by Table 34 and Table 35.

Overall, the purpose of this research question was to identify how a recent graduate would describe, if any, non-technical skill strengths and gaps commonly experienced in Christian cybersecurity undergraduate programs. Based on this research there is a strong trend of recent cybersecurity graduates that are satisfied with their non-technical development.

**Conclusions for Research Question #3**

The participants were presented with a request (Question WP.1) to share if they are satisfied with whole-person development their institution helped them develop. 5 participants responded in a positive manner (e.g., “Yes”, or “Satisfied”). While 1 responded with “It was ok” and another responded with “Not really because of the school specifically”. According to this research, the participants are more satisfied with their whole-person development compared to technical development; however, are less satisfied with their whole-person development compared to non-technical development. This is supported by Table 37.

The participants were asked to go into further details explaining their satisfaction level (Question WP.2). The majority of participants (4) responded in a manner that did not describe any desire for the institution to provide more whole-person development. To further support this.
Zoho’s sentiment analysis indicated 4 participants responded with happy sentiment, 2 participants responded with disappointed sentiment, and 1 participant responded with neutral sentiment. This conclusion is supported by Table 38 and Figure 9.

The participants were asked to share how time was spent regarding whole-person development (Question WP.3). 4 participants responded with “connecting/community/friendship/interaction” with “cyber majors, other undergraduates, residence directory, or faculty”. 2 participants responded with “Biblical classes”. This is supported by Table 39.

The participants were asked (Question WP.4) to discuss any strengths regarding whole-person development at their institution. “Leadership development” was the only strength indicated by 2 participants. This is supported by Table 40.

The participants were asked (Question WP.5) to discuss any gaps regarding whole-person development at their institution. 5 participants responded with “no gaps”. 2 participants shared very strong criticism regarding gaps within their institution. 1 participant responded with “occasional ostracizing non-Christians/lack of loving people”. 1 participant responded with “disconnect between directors and students”, “interested in dishing out consequences”, “lack of grace”, and “not touch a heart”. This is supported by Table 41.

The participants were presented with a request (Question WP.6) to share if they are satisfied with whole-person development their institution helped them develop as it relates to their current job role and industry. There was a slight drop-off compared to the general satisfaction of whole-person development (instead of relating to current job role and industry). 4 participants responded positively with “Yes” or “Satisfied”, 2 participants responded negatively
with “No”, and 1 participant responded with “I can’t see a correlation”. This is supported by Table 42.

The participants were presented with a request (Question WP.9) to any strengths regarding whole-person development their institution helped them develop as it relates to their current job role and industry. 3 participants responded with “none”, “doesn’t really relate”, or “N/A”. “Faith” was the only strength responded by multiple (2) participants. This is supported by Table 45.

The participants were presented with a request (Question WP.10) to any gaps regarding whole-person development their institution helped them develop as it relates to their current job role and industry. 6 participants responded with either “none”, “N/A”, or a similar response. The following items were mentioned by the remaining 1 participant: “group projects”, and “lack of learning how to work together effectively”. This is supported by Table 46.

Besides “ethics/morals” there was not a whole-person item that was identified by multiple participants that they would want present within a cybersecurity program. This is supported by Table 47 and Table 48.

The participants were presented with a request (Question WP.13) to address Biblical whole-person development they encountered at their institution. 4 participants responded with various strengths (e.g., faithfulness, steadfastness, love, compassion, strength, stand strong in faith). 2 participants responded with “Not really” or “Not necessarily”. 1 participant’s response was extremely alarming “college lacks in nearly all of those Biblical whole-person traits”.

The participants were presented with a request (Question WP.14) to discuss anything else related to strengths or gaps regarding whole-person development experienced at their institution. 4 participants responded with “No” or “None”. 1 participant responded positively with “faculty
opening with word of prayer” and “Biblical passage discussion”. 2 participants responded in a negative manner. 1 participant responded negatively with “Relating cyber to Bible/Jesus makes no sense” and “everyone uses openbible.com and mashes verses that are taken out of context”. This participant also challenges faculty to “find a better way to relate cyber to Christian life”. 1 participant responded negatively by stating “good role models are few and not running the college”. This is supported by Table 50.

Overall, the purpose of this research question was to identify how a recent graduate would describe, if any, whole-person strengths and gaps commonly experienced in Christian cybersecurity undergraduate programs. Based on this research there is a strong trend of recent cybersecurity graduates that are satisfied with their whole-person development.

**Conclusions for Research Question #4**

The participants were presented with a request (Question C.1) to share in a 125-250-word essay their cumulative (increasing by successive additions) experience during their cybersecurity undergraduate experience. 4 participants responded with happy sentiment, 2 participants responded with disappointment sentiment, and 1 participant responded with anger sentiment, and 1 participant responded with extremely happy sentiment. Zoho’s sentiment analysis can be found in Figure 10. Table 51 showcases 3 participants responded with the lack of hands-on material within their Christian cybersecurity program experience. 3 participants noted their program was not very “technical”; however, 2 of the 3 did not see that as a negative. 2 participants mentioned they appreciated the “whole person” development they experienced at their institution. 1 participant stated each class was stand-alone. 1 participant responded how the program should help students better prepare for the workforce. 2 participants responded with the feeling the
institution either “lied” or was “shameful” with their business practices. 3 participants responded in a manner that showed appreciation for their faculty/staff.

Overall, the purpose of this research question was to identify how a recent graduate would describe, if any, cumulative strengths and gaps commonly experienced in Christian cybersecurity undergraduate programs. Based on this research there was not a strong trend of cumulative strengths or gaps identified across the recent cybersecurity graduates.

**Implications**

The implications of the research findings will now be highlighted. These implications will attempt to identify areas within the holistic experience of Christian undergraduate cybersecurity students that should be examined by current leaders at their respective programs. These leaders should be able to identify if these research implications are applicable to their current holistic experience they are providing current students and offering future students.

**Implications for Research Question #1**

The data collected regarding the 13 technical section questions (Appendix J) implied the only strengths were either faculty knowledge or external resources (certifications or hands-on (CTFs)). No participants identified any technical curriculum or labs developed by the institution as a strength. This is a technical gap cybersecurity students delimited within this research are facing and should be addressed. One participant mentioned their institution is at the early stages of their cyber range. This gap of the lack of internal development of technical curriculum may have already been identified by this institution. Further research should be conducted to identify if the cyber range removed this technical gap and became a technical strength of this Christian cybersecurity undergraduate program’s experience. The data collected implied that cybersecurity students from Christian institutions are currently more likely to land a cybersecurity job in a
technical role. The data collected also implied that cybersecurity students from Christian institutions are currently more likely to be least satisfied with their technical experience from their institution as compared to non-technical and/or whole-person experiences. Lastly, the data implied that leaders within Christian cybersecurity programs are more likely to find gaps (instead of strengths) within their students’ technical experience.

**Implications for Research Question #2**

The data collected regarding the 13 non-technical section questions (Appendix K) implied primary strengths were ethics/morals and faculty knowledge. The majority of graduates stated there were no gaps in their non-technical experience. The data implied slight gaps (potentially within a specific program) that were identified by a participant were few; however, should be examined: “frameworks”, “assessments”, “security controls”, “lack of preparation for the workforce”, and “hardening”. “Policies, standards, and frameworks” were also mentioned by a participant as a strength. This may be an example of a strength at one program and a gap at another program that is not an overall trend. The data collected implied that cybersecurity students from Christian institutions are currently less likely to land a cybersecurity job in a non-technical role, as compared to a technical role. The data collected also implied that cybersecurity students from Christian institutions are currently more likely to be satisfied with their non-technical experience from their institution as compared to technical experience. The data collected did not imply if cybersecurity students from Christian institutions are currently more or less likely to be satisfied with their non-technical experience from their institution as compared to whole-person experience. Lastly, the data implied that leaders within Christian cybersecurity programs are more likely to find strengths (instead of gaps) within their students’ non-technical experience.
Implications for Research Question #3

The data collected regarding the 14 whole-person section questions (Appendix L) implied the primary strengths that were mentioned across all participants were “connecting/community/friendship/interaction” with “cyber majors, other undergraduates, residence directory, or faculty”, “Biblical classes”, “leadership development”, and “faith”. The data implied slight gaps (potentially within a specific program) that were identified by a participant were few; however, should be examined: “gender inclusion”, “non-Christian inclusion”, “interpersonal skills”, and “practicing the faith from a business perspective”. These gaps should be examined by current Christian cybersecurity programs and self-assess if their institution has these gaps; however, these gaps do not appear to be across both colleges within this research. The data collected also implied that cybersecurity students from Christian institutions are currently more likely to find their whole-person experience to be least applicable to their current work role as compared to technical and non-technical experiences. The data collected did not imply if cybersecurity students from Christian institutions are currently more or less likely to be satisfied with their whole-person experience from their institution as compared to non-technical experience. Lastly, the data implied that leaders within Christian cybersecurity programs are more likely to find strengths (instead of gaps) within their students’ whole-person experience.

Implications for Research Question #4

The data collected regarding the cumulative section question (Appendix M) implied this research question was not answered as there were not enough responses that addressed the concept of cumulative learning. One reason for not getting the responses is due to the clarity of the question. This researcher could have done a better job clearly articulating the definition of
cumulative and shaped the question in an improved manner. It should also be noted that this question was the final question of a lengthy survey and fatigue could have played a factor. These essays should still be examined by current Christian cybersecurity programs and self-assess if their institution related; however, these essays do not directly answer the research question of cumulative learning. For example, inapplicable to Research Question #4, the data collected regarding the cumulative section question (Appendix M) implied multiple participants showed appreciation for their faculty while other participants responded with the feeling the institution either “lied” or was “shameful” with their business practices.

Applications

The applications of this research will now be highlighted. The purpose of the study is to gain an understanding of the perspectives of recent Christian college and university cybersecurity graduates regarding the holistic experience (technical, non-technical, and whole-person) strengths and shortcomings (if any) of their undergraduate academic program as preparation for the workforce. If the experiences of graduates of Christian undergraduate cybersecurity programs are not heard and evaluated by decision-makers of Christian undergraduate cybersecurity programs, how can the experiences of the cybersecurity student improve? Leaders within Christian undergraduate cybersecurity programs can apply this research by drawing from the conclusions and implications previously discussed and reaching out to their graduates regarding their unique technical, non-technical and whole-person experiences during their undergraduate academic journey. This research only highlights a small sample size of the wider audience of Christian cybersecurity undergraduate program graduates that are currently in the workforce. Strengths and gaps were identified within this research. Institutions should take this data as an indicator that even though cybersecurity graduates that are seeking employment are finding a job
does not indicate that the program does not have gaps. These gaps should be examined and addressed. The strengths should also be highlighted and improved upon to further advance the satisfaction of cybersecurity student experiences.

**Research Limitations**

The study applied certain limitations to scope the research towards cybersecurity-specific degrees and work roles to provide accurate conclusions. The first limitation was this study was only available to private colleges that are members of the Council for Christian Colleges & Universities (CCCU), recognized as a Creation College by Answers in Genesis, and/or a Protestant Christian institution by viewing their website and/or mission/faith statement(s). It did not include public institutions, nor private and/or non-Protestant Christian religious institutions (including Catholic institutions). The second limitation was this study was only available to institutions that have a brick-and-mortar presence and are headquartered in the United States. It did not include institutions that are based in a territory of the United States of America nor outside of the United States of America. The third limitation was the participants must have graduated with a four-year degree in cybersecurity (or similar field, e.g., information security, computer security, etc.) from a Christian institution that meets the above requirements. It did not include more common degrees such as computer science and other technology and/or computer-centric degrees where the term ‘security’ is not in the major. It also excluded minors in cybersecurity (or a similar field) when the major does not meet the above requirement. Finally, the fourth limitation was the participants have been employed full-time in the cybersecurity workforce no more than five full years after graduation and are currently employed in a cybersecurity role.
Further Research

To this researcher’s knowledge, there has not been widespread research performed measuring the effectiveness of Christian cybersecurity programs and their impact amongst recent graduates that are now in the workforce. This research to better understand the perspective of recent graduates regarding their Christian undergraduate cybersecurity experience is the first step in measuring Christian cybersecurity programs and their effectiveness. A research opportunity that exists is to perform a case study of one, or multiple, Christian cybersecurity programs to gain a better understanding and improved vantage point of the experiences the participants have discussed within this study.

Another research opportunity would be to research students that have been in the workforce for over 3 years. After a few years in the workforce, the participants may have a different viewpoint of their Christian undergraduate cybersecurity program. Soliciting these participants via social media and other electronic medium methods proved to be minimally effective to gain participation. A different approach should be utilized to reach this demographic, such as going through the academic leader and decision-maker of the alma mater.

More focus and attention could have been given to the cumulative experience of the participants. This could strengthen the conclusions found regarding Research Question #4.

Additionally, this same research and survey could be utilized to understand the student perspective of recent graduate students of Christian graduate cybersecurity programs. This research solicited a highly technical audience; however, the graduate level may solicit a more diverse audience regarding technical and non-technical current work roles.

Furthermore, it was the original intent of this researcher to gain approval from multiple Directors (or equivalent decision-makers) of multiple programs. However, this researcher was
unable to gain approval from multiple Directors after reaching out multiple times via email.

Gaining Director approval could have increased the participant count and institution count of this research. Gaining Director approval should be an avenue to consider for future research for improved response numbers. Gaining access to more participants in a formal setting can lead to adding additional techniques such as member checking and peer debriefing.

Lastly, this research only surveyed participants that are currently in a cybersecurity role. During this research several participants did not meet the requirements due to not being in a cybersecurity role (even though they have a four-year cybersecurity degree). These participants were currently hired in non-cybersecurity-related work roles. Their experiences should also be taken into consideration to gain a better understanding of all students that graduated from a Christian undergraduate cybersecurity program. Were they not prepared well enough to land a full-time role or is there a different reason they are not in this much-needed field?

**Summary**

This study was designed to create a feedback loop that spanned multiple Christian institutions. This research will allow Christian cybersecurity program leaders to self-assess if their programs have any of the strengths or gaps, if identified, to allow their own program to continue to improve or change any shortcomings. The data collected gave personal and practical information regarding the graduate’s Christian undergraduate cybersecurity experience. While the job market has a zero-percent unemployment rate, current cybersecurity programs are vulnerable to assuming their programs are meeting the needs of the students and the workforce when the workforce is starving for talent and all cybersecurity professionals are hired. Analyzing the effectiveness of these programs before either the demand for cybersecurity entry-level professionals drops, or companies decide against hiring cybersecurity professionals after their
undergraduate journey is complete at certain institutions, will better protect current and future students within this four-year cybersecurity developmental pipeline to be optimally prepared for their place in the workforce. While the number of participants was not as high as originally intended, this research instrument is still of value to have comparative data for Directors to reference their own programs and use this research instrument in the future when different students graduate from newer programs (Anderson University, SC, 2019; Bob Jones University, 2019; North Greenville University, 2020; Pensacola Christian College, 2019). This research is a stepping stone to ensuring Christian cybersecurity programs are preparing for the future and not solely taking advantage of the desperate needs the workforce currently has.
REFERENCES


Anderson University, SC. (2019). *Anderson University launching Center for Cybersecurity.* https://andersonuniversity.edu/news/center-for-cybersecurity

Anderson University, SC. (2021a) *Cybersecurity Team Places High in National Competition.* https://andersonuniversity.edu/news/cybersecurity-spring-competition

Anderson University, SC. (2021b) *Anderson Team Consistently Excels in National Cyber League Competition.* https://andersonuniversity.edu/news/anderson-team-consistently-excels-national-cyber-league-competition


CTFtime (2021) *What is capture the flag?* https://ctftime.org/ctf-wtf/


https://transparencyreport.google.com/https/overview


APPENDIX A
FIVE TECHNICAL CORE KNOWLEDGE UNITS (KUS)

- Basic Cryptography
- Basic Networking
- Basic Scripting and Programming
- Network Defense
- Operating Systems Concepts
APPENDIX B
FIVE NON-TECHNICAL CORE KNOWLEDGE UNITS (KUS)

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

[Date]

[Recipient]
[Title]
[Company]
[Address]

Dear ________________:

As a graduate student in the John W. Rawlings School of Divinity at Liberty University, I am conducting research as part of the requirements for a doctoral degree in Christian Leadership. The title of my research project is Understanding Student Perspective of Undergraduate Cybersecurity Programs and Experiences Across Christian Colleges and Universities. The purpose of my research is to gain an understanding of the perspectives of recent Christian college and university cybersecurity graduates regarding the holistic experience (technical, non-technical, and whole-person) strengths and shortcomings (if any) of their undergraduate academic program as preparation for the workforce. This survey will attempt to capture and analyze positive and negative trends that students experienced at their Christian cybersecurity program collegiate experience.

I am writing to request your permission to conduct my research using your graduates at [program] along with other Christian undergraduate cybersecurity programs. The data will be used to better understand the holistic experience cybersecurity graduates experienced including technical skills, non-technical skills, and whole-person development. The privacy of the participants and institutions will be protected. I am requesting for you, as a trusted leader and mentor, to forward the Recruitment Letter and Consent Form to your undergraduate cybersecurity graduates that have graduated during the past five years. Participants will be presented with informed consent information prior to participating. Taking part in this study is completely voluntary, and participants are welcome to discontinue participation at any time. The participants will be asked to take part in a survey regarding their technical, non-technical, and whole-person experience at your Christian undergraduate cybersecurity program.

If you choose to grant permission, a permission letter document is attached for your convenience to complete, sign, and return to me.

I would also like to invite you to serve on the expert panel to review the survey and provide insight prior to the graduates receiving the survey. If you would accept this invitation, please check the applicable box on the permission letter document.

Thank you for considering my request.

Your friend,
APPENDIX E
PERMISSION LETTER

[Date]

Brandon P. Grech
Doctoral Candidate
[Address 1]
[Address 2]

Dear Brandon:

After careful review of your research proposal titled Understanding Student Perspective of Undergraduate Cybersecurity Programs and Experiences Across Christian Colleges and Universities, I have decided to grant you permission to conduct your study at [program].

Check the following box(es), as applicable:

__ I request a copy of the overall results for my institution upon study completion and/or publication.

__ I would like to serve on the expert panel and provide insight to the survey questions.

Sincerely,

Educational Leader’s Name
Educational Leader’s Institution’s Name
Educational Leader’s Institution’s Address
Educational Leader’s Phone Number or Email Address
Dear fellow cybersecurity professional:

As a graduate student in the John W. Rawlings School of Divinity at Liberty University, I am conducting research as part of the requirements for a doctoral degree in Christian Leadership. The purpose of my research is to gain an understanding of the perspectives of recent Christian college and university cybersecurity graduates regarding the holistic experience, (technical, non-technical, and whole-person) strengths, and shortcomings (if any) of their undergraduate academic program as preparation for the workforce. I am writing to invite eligible participants to join my study.

Participants must have graduated with a four-year degree in cybersecurity (or similar degree) from a US-based Christian institution within the last 5 years and be currently employed full-time in a cybersecurity role for at least 3 months but no more than 5 years. Participants, if willing, will be asked to complete a 47-question survey which should take approximately 45 minutes to complete. Participation will be anonymous, and no identifying information will be collected.

To participate, please click here: [Zoho link was placed here]

A consent document is provided as the first page of the survey. The consent document contains additional information about my research. After you have read the consent form, please click the button to proceed to the survey. Doing so will indicate that you have read the consent information and would like to take part in the survey. You do not need to sign the consent form unless you choose to so.

Participants that complete the survey in its entirety will receive instructions on how to claim a $25 Visa Gift Card.

Your friend,

Brandon P. Grech, CISSP, GCFA, GPEN, GSEC
Doctoral Student, Liberty University
APPENDIX G
CONSENT FORM

Title of the Project: Understanding Student Perspective of Undergraduate Cybersecurity Programs and Experiences Across Christian Colleges and Universities
Principal Investigator: Brandon Grech, CISSP, GCFA, GPEN, GSEC, Liberty University

Invitation to be Part of a Research Study
You are invited to participate in a research study. To participate, you must have graduated with a four-year degree in cybersecurity (or similar degree) from a US-based Christian institution within the last five years and be currently employed full-time in a cybersecurity role. Taking part in this research project is voluntary.

Please take time to read this entire form and ask questions before deciding whether to take part in this research.

What is the study about and why is it being done?
The purpose of the study is to gain an understanding of the perspectives of recent Christian college and university cybersecurity graduates regarding the holistic experience (technical, non-technical, and whole-person) strengths and shortcomings (if any) of their undergraduate academic program as preparation for the workforce.

What will happen if you take part in this study?
If you agree to be in this study, I will ask you to do the following:
1. Complete a 47-question survey and should take approximately 45 minutes to complete.

How could you or others benefit from this study?
Benefits to society include helping faculty and leadership at Christian undergraduate programs better understand how recent graduates are satisfied with the holistic experience. This will help faculty and leadership improve their program and better prepare current and future students.

What risks might you experience from being in this study?
The risks involved in this study are minimal, which means they are equal to the risks you would encounter in everyday life.

How will personal information be protected?
The records of this study will be kept private. Published reports will not include any information that will make it possible to identify a subject. Research records will be stored securely, and only the researcher will have access to the records. Data collected from you may be shared for use in future research studies or with other researchers. If data collected from you is shared, any information that could identify you, if applicable, will be removed before the data is shared.

- The privacy of the participants will be protected. Participants and their institution will be assigned a pseudonym. I will conduct the research and analysis where others will not be able to view the unprotected data.
APPENDIX F (Continued)

- Data will be stored on a password-locked computer and may be used in future presentations. The data will be backed up to two external hard drives. Any paper documentation will be protected in a code-protected, fireproof safe.

<table>
<thead>
<tr>
<th>How will you be compensated for being part of the study?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participants will be compensated for participating in this study. Participants that complete the survey in its entirety will receive a $25 Visa Gift Card. Directions to receive your compensation anonymously will be provided after submitting the survey.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Is study participation voluntary?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participation in this study is voluntary. Your decision whether or not to participate will not affect your current or future relations with Liberty University. If you decide to participate, you are free to not answer any question or withdraw at any time prior to submitting the survey without affecting those relationships.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What should you do if you decide to withdraw from the study?</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you choose to withdraw from the study, please exit the survey and close your internet browser. Your responses will not be recorded or included in the study.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Whom do you contact if you have questions or concerns about the study?</th>
</tr>
</thead>
<tbody>
<tr>
<td>The researcher conducting this study is Brandon Grech. You may ask any questions you have now. If you have questions later, you are encouraged to contact him at [redacted]. You may also contact the researcher’s faculty sponsor, Dr. Gary Bredfeldt, at [redacted].</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Whom do you contact if you have questions about your rights as a research participant?</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you have any questions or concerns regarding this study and would like to talk to someone other than the researcher, you are encouraged to contact the Institutional Review Board, 1971 University Blvd., Green Hall Ste. 2845, Lynchburg, VA 24515 or email at <a href="mailto:irb@liberty.edu">irb@liberty.edu</a>.</td>
</tr>
</tbody>
</table>

*Disclaimer: The Institutional Review Board (IRB) is tasked with ensuring that human subjects research will be conducted in an ethical manner as defined and required by federal regulations. The topics covered and viewpoints expressed or alluded to by student and faculty researchers are those of the researchers and do not necessarily reflect the official policies or positions of Liberty University.*

<table>
<thead>
<tr>
<th>Your Consent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before agreeing to be part of the research, please be sure that you understand what the study is about. If you have any questions about the study later, you can contact the researcher using the information provided above.</td>
</tr>
</tbody>
</table>
APPENDIX H
CONSENT FORM AGREEMENT QUESTION

I have read the attached Consent Form, agree to partake in this anonymous survey, and am aware that I will receive a $25 Visa Gift Card for my submission.

[Consent Form]

It can also be viewed HERE [redacted] at this Microsoft OneDrive shared location.
APPENDIX I
QUALIFIER QUESTION

Have you graduated with a four-year (bachelor's) degree in cybersecurity from a Christian institution between January 1st 2016 - August 31st 2021? Similar degrees (e.g., information security, computer security, network security, etc.) are acceptable.
APPENDIX J
QUALIFIER DETAILS QUESTIONS

1. What institution did you graduate from?

2. When did you graduate with your four-year cybersecurity-related degree from a Christian institution?

3. What is the type and the official name of your degree?

4. Describe how long you have been working in cybersecurity full-time since graduation.

5. Describe the industry and current work you perform.

6. Describe your satisfaction with your current work role.
APPENDIX K
TECHNICAL SECTION QUESTIONS

1. Are you satisfied with the technical knowledge and skills your institution helped you develop?

2. Please describe in more detail your satisfaction level with the technical knowledge and skills your institution helped you develop.

3. Please describe if your institution spent more time teaching cybersecurity technical knowledge or technical skills. Please describe how this time was spent.

4. Please describe any strengths at your cybersecurity program, if any, regarding the technical knowledge and skills your institution helped you develop.

5. Please describe any gaps at your cybersecurity program, if any, regarding any technical knowledge and skills you may not have developed.

6. Are you satisfied with the technical knowledge and skills your institution helped you develop as it relates specifically to your current job role and industry?

7. Please describe in more detail your satisfaction level with the technical knowledge and skills your institution helped you develop as it relates specifically to your current job role and industry.

8. Please describe if your institution spent more time teaching cybersecurity technical knowledge or technical skills as it relates specifically to your current job role and industry. Please describe how this time was spent.

9. Please describe if your institution spent more time teaching cybersecurity technical knowledge or technical skills as it relates specifically to your current job role and industry. Please describe how this time was spent.

10. Please describe any strengths at your cybersecurity program, if any, regarding any technical knowledge and skills you developed as it relates specifically to your current job role and industry.

11. Please describe any gaps at your cybersecurity program, if any, regarding any technical knowledge and skills you may not have developed as it relates specifically to your current job role and industry.

12. If you were to create a cybersecurity undergraduate experience, what technical knowledge and skills would you ensure were present in your program that you experienced?

13. Is there anything else you would like to share regarding describing, if any, technical skill strengths and/or gaps you experienced at your cybersecurity undergraduate program?
APPENDIX L

NON-TECHNICAL SECTION QUESTIONS

1. Are you satisfied with the non-technical knowledge and skills your institution helped you develop?

2. Please describe in more detail your satisfaction level with the non-technical knowledge and skills your institution helped you develop.

3. Please describe if your institution spent more time teaching cybersecurity non-technical knowledge or non-technical skills. Please describe how this time was spent.

4. Please describe any strengths at your cybersecurity program, if any, regarding the non-technical knowledge and skills your institution helped you develop.

5. Please describe any gaps at your cybersecurity program, if any, regarding any non-technical knowledge and skills you may not have developed.

6. Are you satisfied with the non-technical knowledge and skills your institution helped you develop as it relates specifically to your current job role and industry?

7. Please describe in more detail your satisfaction level with the non-technical knowledge and skills your institution helped you develop as it relates specifically to your current job role and industry.

8. Please describe if your institution spent more time teaching cybersecurity non-technical knowledge or non-technical skills as it relates specifically to your current job role and industry. Please describe how this time was spent.

9. Please describe if your institution spent more time teaching cybersecurity non-technical knowledge or non-technical skills as it relates specifically to your current job role and industry. Please describe how this time was spent.

10. Please describe any strengths at your cybersecurity program, if any, regarding any non-technical knowledge and skills you developed as it relates specifically to your current job role and industry.

11. Please describe any gaps at your cybersecurity program, if any, regarding any non-technical knowledge and skills you may not have developed as it relates specifically to your current job role and industry.

12. If you were to create a cybersecurity undergraduate experience, what non-technical knowledge and skills would you ensure were present in your program that you experienced?
APPENDIX L (Continued)

13. Is there anything else you would like to share regarding describing, if any, non-technical skill *strengths* and/or *gaps* you *experienced* at your cybersecurity undergraduate program?
APPENDIX M
WHOLE-PERSON SECTION QUESTIONS

1. Are you satisfied with the whole-person development your institution helped instill within you? Whole-person may include personal, spiritual, or other non-cybersecurity development.

2. Please describe in more detail your satisfaction level with the whole-person development your institution helped instill within you.

3. Please describe how your institution spent time with your whole-person development.

4. Please describe any strengths, if any, regarding the whole-person development your institution helped instill within you.

5. Please describe any gaps at your institution, if any, regarding any whole-person development that may not have been instilled within you.

6. Are you satisfied with the whole-person development your institution helped instill within you as it relates specifically to your current job role and industry?

7. Please describe in more detail your satisfaction level with the whole-person development your institution helped instill within you as it relates specifically to your current job role and industry.

8. Please describe how your institution spent time with your whole-person development as it relates specifically to your current job role and industry.

9. Please describe any strengths, if any, regarding your whole-person development your institution helped instill within you as it relates specifically to your current job role and industry.

10. Please describe any gaps at your institution, if any, regarding any whole-person development that may not have been instilled within you as it relates specifically to your current job role and industry.

11. If you were to create a cybersecurity undergraduate experience, what whole-person development would you ensure were present in your program that you experienced?

12. If you were to create a cybersecurity undergraduate experience, what whole-person development would you ensure were present in your program that you did not experience?

13. Using Philippians 4:8, Matthew 5:8, 1 Timothy 4:12, and 1 Corinthians 16:13-14 as references, did you specifically experience any strengths or weaknesses at your institution with these Biblical whole-person traits: speech, conduct, love, faith, purity, strength; steadfastness; faithfulness; and/or being on guard? Feel free to elaborate on other Biblical whole-person traits you may or may not have experienced.
APPENDIX M (Continued)

14. Is there anything else you would like to share regarding describing, if any, whole-person skill strengths and/or gaps you experienced at your cybersecurity undergraduate program?
APPENDIX N
CUMULATIVE SECTION QUESTION

Finally, how would you describe your cumulative (increasing by successive additions) experience during your cybersecurity undergraduate experience? Please describe with a 125-250-word essay.
APPENDIX O
COMPENSATION DELIVERY OPTIONS

1. Email [redacted] (anonymously, if you'd like) an email address or physical address you would like the gift card sent to.

2. Text Brandon at [redacted] (anonymously, if you'd like) an email address or physical address you would like the gift card sent to.

3. Enter your email address or physical address you would like the gift card sent to in this anonymous Zoho survey: [redacted]
APPENDIX P
ALL SURVEY QUESTIONS

Qualifier Details Section:

1. Have you graduated with a four-year degree in cybersecurity from a Christian institution? Similar degrees (e.g., information security, computer security, network security, etc.) will be acceptable. If yes, what is the title of your degree?

2. What institution did you graduate from?

3. When did you graduate (month and year)?

4. Describe how long you have been working in cybersecurity full-time since graduation.

5. Describe the industry and current work you perform.

6. Describe your satisfaction with your current work role.

Technical Section Questions:

1. Are you satisfied with the technical knowledge and skills your institution helped you develop?

2. Please describe in more detail your satisfaction level with the technical knowledge and skills your institution helped you develop.

3. Please describe your institution’s time allocation teaching cybersecurity technical knowledge versus skills. Please describe how this time was spent.

4. Please describe any strengths, if any, regarding the technical knowledge and skills your institution helped you develop.

5. Please describe any gaps at your cybersecurity program, if any, regarding any technical knowledge and skills you may not have developed.

6. Are you satisfied with the technical knowledge and skills your institution helped you develop as it relates specifically to your current job role and industry?

7. Please describe in more detail your satisfaction level with the technical knowledge and skills your institution helped you develop as it relates specifically to your current job role and industry.

8. Please describe your institution’s time allocation teaching cybersecurity technical knowledge versus skills as it relates specifically to your current job role and industry. Please describe how this time was spent.
9. Please describe any strengths, if any, regarding the technical knowledge and skills your institution helped you develop as it relates specifically to your current job role and industry.

10. Please describe any gaps at your cybersecurity program, if any, regarding any technical knowledge and skills you may not have developed as it relates specifically to your current job role and industry.

11. If you were to create a cybersecurity undergraduate experience, what technical knowledge and skills would you ensure were present in your hypothetical program that you experienced at your own undergraduate experience?

12. If you were to create a cybersecurity undergraduate experience, what technical knowledge and skills would you ensure were present in your hypothetical program that you did not experience at your own undergraduate experience?

13. If there is anything else you would like to share regarding describing, if any, technical skill strengths and gaps you experienced at your cybersecurity undergraduate program?

Non-Technical Section Questions:

1. Are you satisfied with the non-technical knowledge and skills your institution helped you develop?

2. Please describe in more detail your satisfaction level with the non-technical knowledge and skills your institution helped you develop.

3. Please describe your institution’s time allocation teaching cybersecurity non-technical knowledge versus skills. Please describe how this time was spent.

4. Please describe any strengths, if any, regarding the non-technical knowledge and skills your institution helped you develop.

5. Please describe any gaps at your cybersecurity program, if any, regarding any non-technical knowledge and skills you may not have developed.

6. Are you satisfied with the non-technical knowledge and skills your institution helped you develop as it relates specifically to your current job role and industry?

7. Please describe in more detail your satisfaction level with the non-technical knowledge and skills your institution helped you develop as it relates specifically to your current job role and industry.

8. Please describe your institution’s time allocation teaching cybersecurity non-technical knowledge versus skills as it relates specifically to your current job role and industry. Please describe how this time was spent.
9. Please describe any strengths, if any, regarding the non-technical knowledge and skills your institution helped you develop as it relates specifically to your current job role and industry.

10. Please describe any gaps at your cybersecurity program, if any, regarding any non-technical knowledge and skills you may not have developed as it relates specifically to your current job role and industry.

11. If you were to create a cybersecurity undergraduate experience, what non-technical knowledge and skills would you ensure were present in your hypothetical program that you experienced at your own undergraduate experience?

12. If you were to create a cybersecurity undergraduate experience, what non-technical knowledge and skills would you did not experience at your own undergraduate experience?

13. If there is anything else you would like to share regarding describing, if any, non-technical skill strengths and gaps you experienced at your cybersecurity undergraduate program?

Whole-Person Section Questions:

1. Are you satisfied with the whole-person development your institution helped instill within you?

2. Please describe in more detail your satisfaction level with the whole-person development your institution helped instill within you.

3. Please describe how your institution spent time with your whole-person development.

4. Please describe any strengths, if any, regarding the whole-person development your institution helped instill within you.

5. Please describe any gaps at your institution, if any, regarding any whole-person development that may not have been instilled within you.

6. Are you satisfied with the whole-person development institution helped instill within you as it relates specifically to your current job role and industry?

7. Please describe in more detail your satisfaction level with the whole-person development institution helped instill within you as it relates specifically to your current job role and industry.

8. Please describe how your institution spent time with your whole-person development as it relates specifically to your current job role and industry.
9. Please describe any strengths, if any, regarding your whole-person development your institution helped instill within you as it relates specifically to your current job role and industry.

10. Please describe any gaps at your institution, if any, regarding any whole-person development that may not have been instilled within you as it relates specifically to your current job role and industry.

11. If you were to create a cybersecurity undergraduate experience, what whole-person development would you ensure were present in your hypothetical program that you experienced at your own undergraduate experience?

12. If you were to create a cybersecurity undergraduate experience, what whole-person development would you ensure were present in your program that you did not experience at your own undergraduate experience?

13. Using Philippians 4:8, Matthew 5:8, 1 Timothy 4:12, and 1 Corinthians 16:13-14 as references, did you specifically experience any strengths or weaknesses at your institution with these Biblical whole-person traits: speech, conduct, love, faith, purity, strength; steadfastness; faithfulness; and/or being on guard? Feel free to elaborate on other Biblical whole-person traits you may or may not have experienced.

14. If there is anything else you would like to share regarding describing, if any, whole-person skill strengths and gaps you experienced at your cybersecurity undergraduate program?

Cumulative Section Question:

1. Finally, how would you describe your cumulative (increasing by successive additions) experience during your cybersecurity undergraduate experience? Please describe with a 125-250-word essay.