

CYBERSECURITY IN THE INFORMATION AGE: A CONNECTIVIST APPROACH TO
INSTRUCTIONAL DESIGN; A CASE STUDY

Michael Lance Whisenant

Dissertation Prepared for the Degree of
DOCTOR OF PHILOSOPHY

UNIVERSITY OF NORTH TEXAS

December 2024

APPROVED:

Deborah Cockerham, Major Professor
Bill Elieson, Committee Member
Regina Kaplan-Rakowski Committee
Member

Xun Ge, Chair of the Department of
Learning Technologies

Kinshuk, Dean of the College of Information
Victor Prybutok, Dean of the Toulouse
Graduate School

Whisenant, Michael Lance. *Cybersecurity in the Information Age: A Connectivist Approach to Instructional Design; A Case Study*. Doctor of Philosophy (Learning Technologies), December 2024, 87 pp., 7 tables, 10 figures, 5 appendices, references, 69 titles.

This case study explores the effects of an introductory cybersecurity education course on participants' cybersecurity knowledge and preparedness. The research questions examine participants' initial perceptions of cybersecurity practices before taking the course and the perceived effectiveness the course had on their cybersecurity preparedness. The study employed a mixed-methods approach, involving 15 participants in a pre-intervention survey and eight participants in a post-intervention focus group discussion. Findings indicate that the course improved participants' knowledge and awareness of the need for actions to support cybersecurity and suggest the need for cybersecurity training that incorporates both technical skills, such as security protocols, and human factors, such as user behavior practices. In addition, participants planned to adopt cybersecurity practices such as using multi-factor authentication (MFA) and password managers, into their regular technology use. This case study lays the groundwork for further research into the design and instructional approach to cybersecurity training, which could potentially inform future educational strategies and policies.

Copyright 2024

by

Michael Lance Whisenant

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my wife, parents, family, and friends for their unwavering support and encouragement throughout this journey. Their belief in me has been a constant source of motivation.

I am profoundly grateful to my Major Professor, Dr. Cockerham, for her invaluable guidance, insight, and patience. Her expertise and mentorship have been instrumental in shaping this dissertation. I would also like to thank my committee members, Dr. Elieson and Dr. Kaplan-Rakowski, for their thoughtful feedback and constructive criticism. Additionally, I extend my sincere thanks to the University of North Texas and Texarkana College for providing the necessary resources and support for my research.

I am also thankful to the participants of my study. Their willingness to share their experiences and insights has been crucial to the success of this research. Lastly, I wish to express my heartfelt appreciation to everyone who has been a part of this journey. This dissertation would not have been possible without you.

TABLE OF CONTENTS

	Page
ACKNOWLEDGEMENTS	iii
LIST OF TABLES	vii
LIST OF FIGURES	viii
CHAPTER 1. INTRODUCTION	1
Overview of the Problem	2
Cybersecurity	2
Brief Historical Overview of Cybersecurity	3
Cybersecurity Threats	6
Need for the Study	11
Educating the User	11
Community College Needs	14
Purpose of the Study	15
Research Questions	16
Overarching Research Questions	16
Outcomes and Contributions to the Body of Knowledge	17
Structure of the Dissertation	17
Delimitations	18
Summary	19
CHAPTER 2. LITERATURE REVIEW	20
Introduction	20
Threat Landscape	20
Threat Implications	21
Foundational Research	23
Resiliency in Cybersecurity	23
National Cybersecurity Agenda	24
Cybersecurity and Curriculum Models	25
Agile Strategies in Curriculum Design	27
Social Cybersecurity	29
Theoretical Framework	30

Connectivism	30
Connectivism Examined	31
Connectivism and NIST	32
Recent Studies.....	32
Critical Infrastructure Security	32
Connective Learning	35
Evidentiary Information.....	36
Summary	37
CHAPTER 3. METHODOLOGY	38
Introduction.....	38
Study Goals	38
Research Questions	39
Research Design.....	39
Quantitative Component	39
Qualitative Component	40
Setting	40
Participants.....	40
Sampling Procedure	40
Target Population.....	41
Recruiting Approach.....	41
Data Collection	42
Pre-Course Survey	42
Focus Group Discussion Questions	42
Data Analysis	42
Data Preparation.....	42
Quantitative Analysis Procedures	43
Qualitative Analysis Procedures	43
Transcription and Coding Process	43
Categorization and Theme Identification.....	44
Validation Procedures	44
Threats to Validity	44
Summary	45

CHAPTER 4. FINDINGS.....	46
Introduction.....	46
Quantitative Results: Research Question 1	46
Overview of the Research Question	46
Demographic Data	46
Survey Data.....	48
Qualitative Results: Research Question 2.....	49
Overview of the Research Question	49
Thematic Analysis Process	50
Analysis of Emergent Themes	51
Summary	55
CHAPTER 5. IMPLICATIONS AND CONCLUSIONS	56
Introduction.....	56
Research Discussion Overview.....	56
Discussion	57
Limitations	60
Future Research	61
Practical Implications.....	62
Theoretical Implications	63
Contributions to the Field	65
Conclusion	65
APPENDIX A. IRB APPROVAL LETTERS	67
APPENDIX B. RECRUITMENT FLYER	70
APPENDIX C. INFORMED CONSENT FOR STUDIES WITH ADULTS	72
APPENDIX D. QUANTITATIVE SURVEY	77
APPENDIX E. FOCUS GROUP QUESTIONS.....	80
REFERENCES	82

LIST OF TABLES

	Page
Table 1. Demographic Data	47
Table 2. Likert Scale Data.....	49
Table 3. Categorical Data.....	49
Table 4. Overall Impressions	52
Table 5. Presentation and Engagement	53
Table 6. Understanding and Application.....	54
Table 7. Usability and Navigation	55

LIST OF FIGURES

	Page
Figure 1. Cybersecurity Components	3
Figure 2. Depiction of a Honeypot	8
Figure 3. Course Modules.....	12
Figure 4. Literature Review Search Results	16
Figure 5. Cybersecurity Hygiene-In-Action	21
Figure 6. Cyber Resilience Core Principles.....	23
Figure 7. Community of Inquiry (COI)	26
Figure 8. Social Cybersecurity.....	29
Figure 9. Framework Functions.....	31
Figure 10. Connectivism and Cybersecurity.....	36

CHAPTER 1

INTRODUCTION

In the domain of cybersecurity education, Payne et al. (2021) presents a persuasive argument for an interdisciplinary approach to course design. The authors contend that the innovation of technology has interconnected our interests and options to such an extent that technological change is affecting our human behaviors. Due to the behavioral shifts caused by technology's pervasive role in our daily lives, there have been increased vulnerabilities, threats, and risks. This situation necessitates educational entities to enhance and introduce more cybersecurity academic programs. While there has been growth in updating and introducing new courses, degrees, and certifications, it might not be at the same rate as the emergence of new employment opportunities (Payne et al., 2021).

In response to this demand, the researchers emphasize a need for cybersecurity education to follow an interdisciplinary and diverse approach that focuses on both the human subject and the technical elements of cybersecurity. This viewpoint is particularly pertinent in our current digital era where cybersecurity threats are not limited to the technical realm but have far-reaching implications for our society. According to the Occupational Outlook Handbook (OOH), as published on the United States Bureau of Labor Statistics' website, the employment of Information Security Analysts is projected to grow by 32% from 2022 to 2032. This growth rate is categorized as "much faster than average" compared to other occupations (U.S. Bureau of Labor Statistics, 2023). To meet the current projected demand, there is a need for cybersecurity education to expand beyond its technical shell and adopt an interdisciplinary educational approach.

Overview of the Problem

Cybersecurity

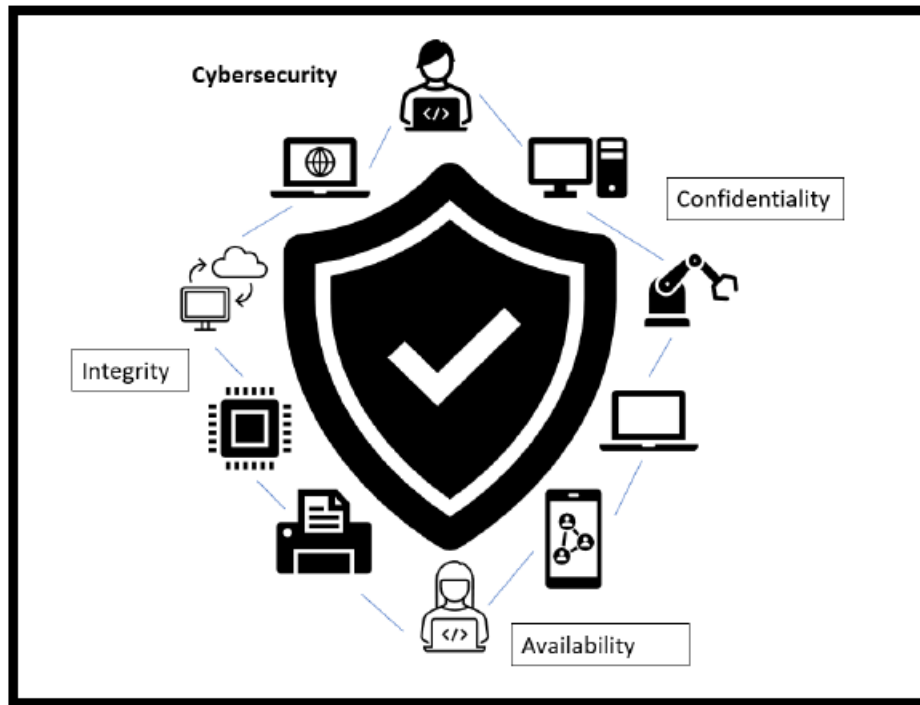
As our reliance on digital platforms and electronic communication continues to grow, understanding and implementing a comprehensive approach to digital security becomes increasingly crucial for organizations and individuals alike. Cybersecurity, as defined by the National Institute of Standards and Technology (NIST), encompasses the “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” (CSRC Content Editor, n.d.). This inclusive definition underscores the multifaceted nature of cybersecurity, emphasizing not only the protection of electronic systems and communications, but also the assurance of the information’s authenticity, confidentiality, and overall integrity. Basie & Rossouw (2018), in contrast, emphasize cybersecurity’s focus on the confidentiality, integrity, and availability of online information, underscoring the specialized nature of cybersecurity within the broader realm of information security. This perspective, while aligning with NIST’s broad definition, zeroes in on the specialized nature of cybersecurity within the broader realm of information security. It highlights the focus on digital assets and the unique challenges posed by internet-based threats which helps enrich our understanding of cybersecurity’s multifaceted domain.

For the purposes of this study, cybersecurity is defined as follows: Cybersecurity refers to the proactive protection and subsequent restoration of digital assets, encompassing electronic communications and the information they contain, to guarantee their confidentiality, integrity, and availability (Basie & Rossouw, 2018; CSRC Content Editor, n.d.). This definition integrates

the broad scope of cybersecurity as identified by NIST with the specific focus on the confidentiality, integrity, and availability of online information as underscored by Basic & Rossouw (2018).

Figure 1

Cybersecurity Components



Brief Historical Overview of Cybersecurity

Funded by the Department of Defense (DOD) in the 1960s and early 1970s, the Advanced Research Projects Agency Network (ARPANET) mission was to demonstrate packet switching's utility to military command and control, especially in the context of nuclear threats (Lukasik 2011). Its goals encompassed ensuring robust control over U.S. nuclear capabilities and refining both strategic and operational military decision-making. While its primary emphasis was on defense, the broader implications of networking for civilian purposes were also acknowledged. As ARPANET developed, it laid the foundation for today's Internet by extending

its influence beyond the U.S. and fostering a growing community of users and pioneers (Lukasik 2011).

In describing this development, Linden (1976) sheds light on the pressing issue of computer-related crimes, emphasizing the substantial financial repercussions stemming from such activities. A significant portion of these crimes can be attributed to internal fraud by employees who have access to digitized financial records. Linden contends that a narrow focus on security, to the exclusion of software reliability, is counterproductive. He further contends that while the costs associated with inadequate security controls are substantial, they are dwarfed by the costs associated with flawed and unreliable software. In addressing both security and reliability, systems can be better equipped to handle the challenges of computer privacy, critical software applications, and the rising costs of software development.

The arrival of a networked environment created a need for a documented set of standards that could be used to secure a system. DoD and the National Bureau of Standards (NBS) were instrumental in their efforts to secure classified information within computer systems. The establishment of DoD Directive 5200.28 and subsequent manuals laid the groundwork for standardized security policies and technical measures, thus reflecting a growing awareness of the need for robust computer security protocols as early as the 1970s (DoD, 1985).

The DoD Computer Security Initiative in 1977 and the formation of the DoD Computer Security Center in 1981 were significant milestones that underscored the commitment to advancing trusted computer systems (DoD, 1985). The criteria emphasized the incorporation of security features that could be created by manufacturers within their commercial products. Additionally, it established a benchmark for the DOD to gauge the dependability of computer systems.

The requirements for a secure information system are built upon six fundamental security principles that ensure only authorized individuals or processes have access to sensitive information and that the security mechanisms of a system are robust and reliable (DoD, 1985).

- *Security policy*: A security policy dictates strict access controls. This ensures only cleared individuals access sensitive data and that selective sharing is based on a defined need-to-know basis.
- *Access control labels*: Objects must have labels that indicate their sensitivity level or access rights to enforce a mandatory security policy effectively.
- *Identification*: Each user's identity and access permissions must be securely managed by the system to control their interactions with sensitive actions and information.
- *Accountability*: The system must securely log and maintain audit records to attribute security actions to specific users and ensure efficient oversight and investigation of breaches.
- *Assurance*: The computer system must have verifiable hardware and software controls to ensure it meets the criteria, with clear evidence available for an independent assessment.
- *Continuous protection*: Security mechanisms must be immune to tampering and unauthorized changes to ensure a system's continuous protection throughout its lifecycle.

As a result of the requirements listed, the DoD created four divisions in a tiered manner that allows the user to determine the level of sensitive information that is safeguarded. Division D establishes the foundational level of protection, while Division C advances this by offering discretionary protection and integrating audit features to uphold accountability (DoD, 1985). Division B enhances the security protocols by implementing a trusted computing base (TCB) that enforces strict access controls and incorporates sensitivity classifications within the system's

fundamental data constructs. Division A, the highest level, demands confirmed security measures through extensive validation processes to ensure the robustness of the system's protective mechanisms (DoD, 1985).

Cybersecurity Threats

The evolution from acknowledging the need for computer security to developing a comprehensive framework for evaluation illustrates the strategic and cooperative approach of government bodies to address the challenges of protecting sensitive data in a digitally connected world. In an innovative approach to intrusion detection strategies, A.K. Dewdney's (1984) computer simulation game, *Core War*, focused on two computer programs engaged in a virtual battle. The game's core feature is that there's no real-time human input in battles. Instead, the pre-set tactics ingrained in the combatants determine the results of the engagements (Dewdney, 1984).

The programs that compete in memory space exhibit different levels of complexity and effectiveness in their operational tactics. A basic program, *Imp*, reproduces a single line of code throughout the memory, whereas another simple program, *Dwarf*, inserts non-executable zeros at every fifth address to interfere with the execution of other programs. *Gemini*, *Juggernaut*, and *Bigfoot* are more advanced programs that employ the same strategy of duplicating themselves at varying intervals ahead of their current position. *Gemini* replicates at a location one hundred addresses forward, as *Juggernaut* makes a copy of itself ten addresses in front of its original location. *Bigfoot* repeats its pattern based on a large prime number sequence. This process complicates the tracking and pinpointing of its position thus earning its fabled name. Lastly, *Raidar* is a sophisticated program that creates protective buffers and launches systematic attacks while detecting and preventing intrusions. *Scanner*'s novelty is due to its ability to maintain two

copies of itself. This allows the program to run while scanning and repairing the other, thus ensuring the integrity of the system.

Dewdney's article showcases how engaging with Core War can be an educational experience as programming principles like loops, conditional execution, and subroutines can be learned through an interactive and competitive digital environment (Dewdney, 1984). Moreover, the article suggests that the tactical approaches in Core War have relevance outside the game and could potentially influence real-world technology (as evidenced in our current society).

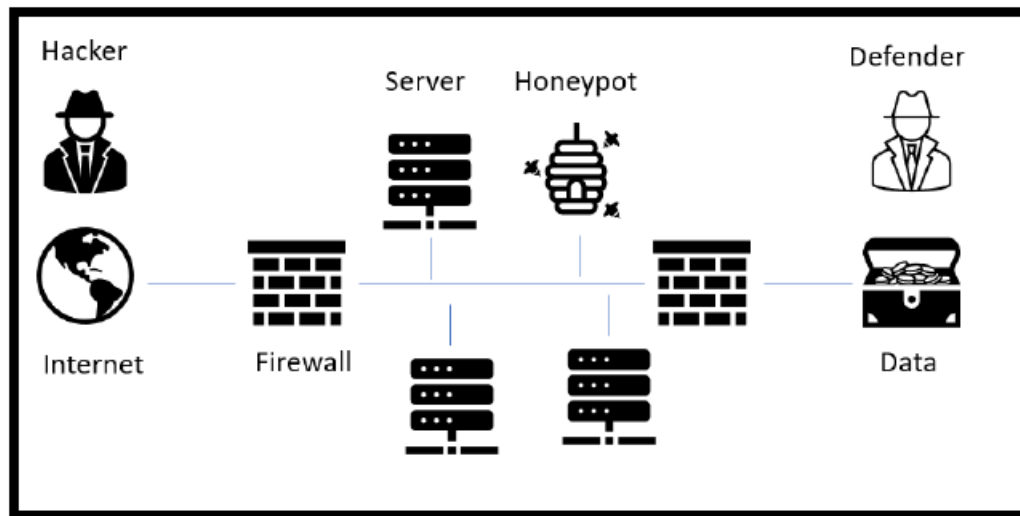
Strategies such as self-replication and autonomous repair are not simply a feature in cyber gameplay as modern malware has shown the ability to adapt and evolve for destructive purposes. Similarly, threat actors have also evolved to take advantage of unguarded systems as demonstrated in Clifford Stoll's (1988) article, *Stalking the Wily Hacker*. This report provides a comprehensive summary of the August 1986 cybersecurity incident on the Lawrence Berkeley Laboratory (LBL). Originally noticed as an accounting error that led to the discovery of an account without a billing address, the researchers soon realized that an intruder was in their system and had obtained system-manager privileges (Stoll, 1988). Rather than tighten their system and expel the trespasser, the team employed the novel approach of continued access as they documented the intruder's activities and traced the source.

Termed a honeypot (see Figure 2) due to its alluring award, the researchers monitored as the intruder used multiple networks, such as ARPANET/MILNET (Military Network), the Magnetic Fusion Energy network, and the High Energy Physics network, to try and enter more than 400 sensitive computers (Stoll, 1988). The intruder's tactics were opportunistic in nature in that common account names, active sessions, and operating systems security holes, were exploited to search file structures for defense and military keywords. Secondly, the intruder

would scan for passwords saved in unencrypted documents. Both tactics, though simplistic, proved to be effective as about 5% of the machines allowed access via default accounts names and passwords (Stoll, 1988).

Figure 2

Depiction of a Honeypot



Note. This figure depicts a honeypot strategy where a decoy system lures hackers away from real servers and data while being monitored by a defender, thus demonstrating an interactive cybersecurity defense mechanism.

In the wake of the security breaches, the LBL embarked on a strategic overhaul of its cybersecurity measures, adopting an approach that married technical safeguards with behavioral change. This included the introduction of password expiration policies to compel regular updates, the deletion of obsolete accounts coupled with a ban on account sharing, and the vigilant monitoring of network traffic with the implementation of alerts for anomalous patterns (Stoll, 1988). Additionally, a concerted effort was made to boost user education in the choosing of unique passwords and the importance of properly safekeeping their credentials.

The insights gleaned from this case study reveal that cybersecurity is not merely a technological choice, but also a human factor challenge in that the behaviors and practices of the user have major ramifications. The researchers further characterized the intruder as a skilled

programmer with knowledge in system administration; while further clarifying that he doesn't possess the extraordinary expertise often depicted in popular imagination (Stoll, 1988). This description of the intruder, later determined to be German hacker Markus Hess, demonstrates the need for improved security education among users and administrators to better understand the threat landscape.

It is within this context of growing awareness and the increasing sophistication of threats that the commercial antivirus industry began to take shape. In 1987, John McAfee established McAfee Associates and launched VirusScan, the company's inaugural antivirus offering (Sahay, 2023). This period marked the beginning of an intensive effort to develop tools that could provide a layer of defense against vulnerable attack surfaces. As a result, antivirus programs were engineered to identify, defend, and neutralize digital threats through various techniques. Signature-based detection, one of the earliest methods, relies on identifying unique patterns associated with known viruses (Samociuk, 2023). Although this method is effective at identifying known threats, it potentially struggles with new or altered malware, resulting in the need for frequent updates to its database. Behavior-based detection techniques entail analyzing the behavior of programs upon execution to determine their intent.

Cohen (1987) introduced behavioral recognition as a method to differentiate between illicit and legitimate services in a system. This approach, in contrast to signature-based detection that searches for specific patterns, identifies threats by grouping programs that exhibit similar behaviors under a behavioral signature (Samociuk, 2023). This type of detection method has the potential to create false positives if benign programs are running resources like known malware. Heuristic-based analysis involves either a static or dynamic methodology in determining the detection of malware. Static heuristic detection scrutinizes the anticipated behaviors of

decompiled code by comparing it with established heuristic patterns, while dynamic heuristic detection observes the actions of a program within a protected and isolated setting (sandbox) to identify any malicious behavior (Li et al., 2021).

As commercial anti-virus software became more popular among personal computer consumers, threat actors were also updating their tactics to try and circumvent the protective methods being used and deployed. On Friday, March 26, 1999, the Melissa virus began spreading through networks via email attachments purported to have come from a known contact. (Garber, 1999). Melissa's relative simplicity and the exploitation of common user behaviors (such as the opening of email attachments) caused concern among professionals tasked with security solutions. Melissa's novelty was that it leveraged the macro language capabilities of Microsoft's Visual Basic for Applications (VBA) to execute malicious functions. This highlighted a significant gap in the protection offered by traditional antivirus methods as signature-based detection could only identify known threats, and Melissa's unique signature was initially unknown to these systems (Garber, 1999). Similarly, the next year, the Love Bug worm, politely addressed as 'kindly check the attached love letter from me,' began circulating among individuals and enterprises. When the attachment was activated, the embedded code began modifying and moving the user's multimedia files. It also redirected the web browser to a site that downloaded another harmful element capable of hijacking and transmitting the computer's saved passwords to an undisclosed destination (Knight, 2001).

The emergence of the Melissa virus and the subsequent Love Bug worm marked a pivotal moment in the evolution of cyber threats. As personal computers became more widespread, individuals were tasked with protecting their digital assets from the influence of threat actors. This shift necessitated a new approach to cybersecurity, one that addressed the unique

vulnerabilities presented by the widespread use of personal computers and the intimate data they held.

Need for the Study

Educating the User

A critical component in this shift is the education of the end user. The Center for Cybersecurity Education and Research (CCER) is located on the campus of Old Dominion University (ODU) and serves as an example case study in cybersecurity education. Founded in 2015, the Center's Cybersecurity, Technology, and Society course was designed by five faculty members from diverse backgrounds and departments: computer engineering, philosophy, computer science, business information technology, and criminal justice (Payne et al., 2021). The five agreed upon themes by the faculty members and research authors served as the guiding principles for the course's development. In short:

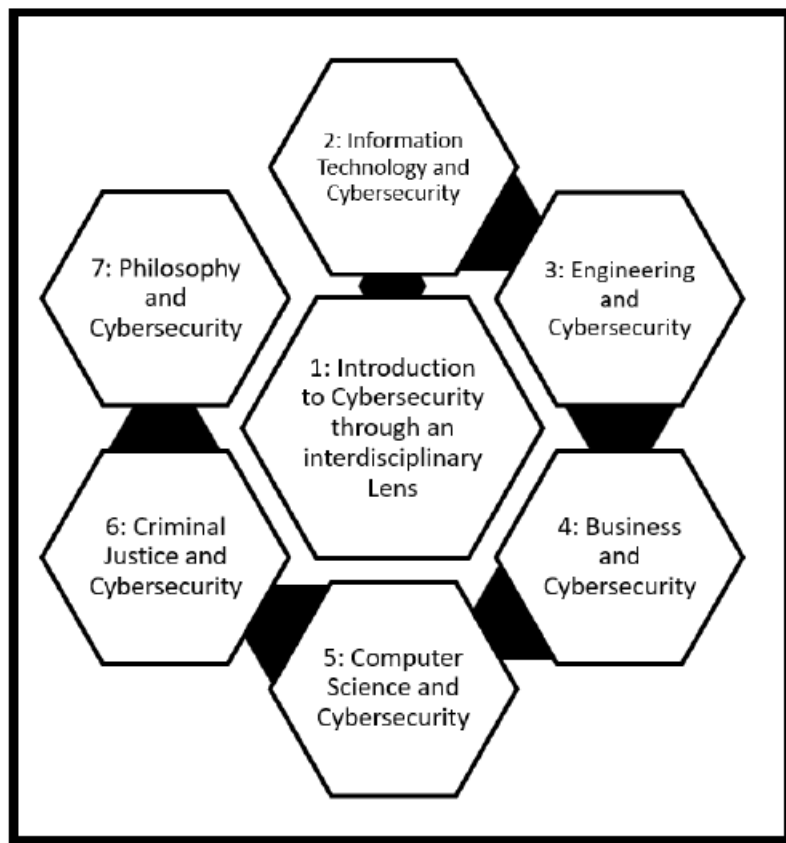
- The course must be grounded in interdisciplinary themes.
- It must be developed in a way that students from various backgrounds would be able to successfully complete the class.
- The course must use open educational resources as reading materials.
- It must be made available in an open format for others to use.
- Each disciplinary area should be equally emphasized through an interdisciplinary lens.

In developing the course, faculty then aligned the learning outcomes (LOs) of the proposed course with the institutional LOs as defined in their general education requirements. The course was established with a focus on exploring the intersection of technology and cybersecurity from a multidisciplinary viewpoint. It aimed to address how cybersecurity issues, driven by technological advancements, intertwine with cultural, political, legal, ethical, and

business aspects (Payne et al., 2021). Seven learning modules were designed with each faculty member contributing a module respective to their field. The first two modules are interdisciplinary as the introductions and definitions are established and the framework is presented. The remaining five modules explore cybersecurity through the view and framework of the specific faculty member's discipline (see Figure 3).

Figure 3

Course Modules



Note. Each hexagon represents a distinct area of focus, demonstrating the multidisciplinary nature of cybersecurity education.

Central to the course, and consistent among the instructors, are the open-ended questions where students are asked to critically think about the questions as their responses are then submitted as assignments for the instructors to evaluate (Payne et al., 2021). Furthermore,

students are tasked with expanding on three of their journal entries and blending the ideas in a way that exhibits a thorough comprehension of the relationships among different cybersecurity subjects (Payne et al., 2021). Consistent with the third theme identified in the course establishment phase, open-educational resources (OER) were used as the primary basis for the reading material. Not only does this framework allow for flexibility and cost-savings, but the information is available to the student at the beginning of the semester (Payne et al., 2021). Referencing open educational resources (OER) potential impact, Whisenant (2022) emphasized the growing impact of OERs such as YouTube and Khan Academy as they are fostering a new breed of learners who are adept at using technology and can absorb large amounts of information (potentially transforming the learning landscape).

Several methods were used to access the course with the initial assessment focused on a review of the learning materials, and a matrix linking institutional learning outcomes with the course's learning outcomes. Secondly, a review of all courses and curriculum by faculty at an assessment summit led to faculty discussions on how to develop strategies for a foundational course that is part of the general education curriculum. As a result, 517 students had completed the course by the Spring 2020 semester, with 169 students being non-majors from the disciplines of criminal justice, psychology, computer science, leadership, and information systems and technology (Payne et al., 2021).

After implementing the study, the authors recommended five strategies for others attempting to develop similar courses. First, they emphasized the value of embracing interdisciplinary approaches, which reflect real-world complexities and nurture critical thinking skills. Second, it is crucial to avoid departmental ownership to maintain a truly interdisciplinary nature. Third, a focused approach is advised, recognizing that introductory courses cannot make

experts but that they should prioritize key learning outcomes. Fourth, educators are encouraged to explore innovative ways to integrate cybersecurity into general education curricula. Finally, they advocate for the prudent use of open education resources and the sharing of course materials to enhance access to interdisciplinary knowledge.

Community College Needs

The curriculum developed by the CCER at Old Dominion University represents a comprehensive, interdisciplinary approach tailored for a research-intensive environment. While the principles and structure of the ODU course offer valuable insights, the specific needs and context of community college students necessitate a different educational approach. Community college students often have varied educational backgrounds, immediate job-oriented goals, and diverse life circumstances that can impact their educational journey (Whisenant & Bradshaw, 2021). The ODU curriculum may not align with a community college whose nontraditional population and open admission standards potentially attracts a student who is often attending college without the needed technological skills (e.g., Byrd and Macdonald, 2005; Wallace and Clariana, 2005; Henson, 2014; Goncalves and Trunk, 2014; Eichelberger and Imler, 2016).

The resources of a public research university such as ODU likely outnumber those which a community college can offer. Community colleges typically focus on imparting practical skills and knowledge that directly translate to the workforce. Furthermore, teaching methods and course content for community college students needs to be accessible and pertinent, especially for those juggling their education with work and other commitments. The incorporation of OERs in the ODU curriculum, however, stands out as especially pertinent and advantageous for community colleges. This approach guarantees immediate access to essential learning materials for all students.

Purpose of the Study

This case study's purpose is to design and evaluate an introductory cybersecurity course (referred to as connected security (CS) in this study) grounded in the connectivism learning theory and the NIST cybersecurity standards. This course also draws inspiration from the Workforce Education Course Manual (WECM) accreditation standards for the Information Technology (IT) Security course (ITSY 1342) for public two-year colleges in Texas. The approved learning outcomes for ITSY 1342 by this organization, which served as guidance when forming the CS course (Texas Higher Education Coordinating Board (THECB), 2022), include:

- Apply National Institute of Standards and Technology (NIST) guidelines and other best practices.
- Develop backup/recovery procedures to provide data security.
- Use desktop /device operating system features to implement security.
- Identify computer and network threats and vulnerabilities and methods to prevent their effects.
- Use tools to enhance network security.
- Use encryption techniques to protect network local and distributed systems data.

Among the learning theories, constructivism appears to be the most researched in the context of both cybersecurity and information security. Gaming, as a pedagogical tool, seems to be a popular topic within this realm. There is a noticeable overlap in results across different search terms, especially when moving from cybersecurity to information security. This overlap suggests that some articles might be using both terms interchangeably and/or are broad enough to encompass both areas. Some learning theories (e.g., connectivism) and models (ADDIE; (analysis, design, development, implementation, and evaluation) instructional design (ID) model have limited or no relevant results, indicating potential gaps involving these methodologies.

Figure 4

Literature Review Search Results

Cybersecurity Lit Review Search Results	Information Security Lit Review Search Results
Total Results: 157	Total Results: 889
Filters Applied:	Filters Applied:
Last 3 years	Last 3 years
Full-text	Full-text
Education discipline	Education discipline
Education subject	Education subject
From the Results:	From the Results:
Cybersecurity + Education: 161 results	Information Security + Education: 889 results
Cybersecurity + Learning Theory: 7 results	Information Security + Learning Theory: 50 results
Cybersecurity + Connectivism:	Information Security + Connectivism: No results
1 result that was not relevant	Information Security + Constructivism: 3 results
Cybersecurity + Constructivism: 17 results	Two overlapping results
Four articles involved gaming (can be used)	One result that was not relevant
One involving eHealth	Information Security + Situated Learning:
10 involving international policy or similar	2 results that were not relevant
One article was a repeat.	Information Security + ADDIE: No results
One article involved Experiential Learning	
Cybersecurity + Self-Directed Learning: 2 results	
One article was relevant and can be used	
Cybersecurity + Situated Learning:	
2 results that were not relevant	
Cybersecurity + ADDIE: 3 results	
One result was relevant	

Note. This figure provides a summary of literature search results comparing the number of sources found on cybersecurity and information security within education. The left side details the results for “Cybersecurity Lit Review” and the right side for “Information Security Lit Review,” including total results, filters applied, and relevant findings by category. This demonstrates the scope and focus areas of current research in these fields.

Research Questions

This case study aims to bridge the identified gaps in literature and practice by developing an introductory cybersecurity curriculum that can be facilitated by interdisciplinary instructors in an online environment.

Overarching Research Questions

- What were participants’ perceptions of cybersecurity practices before taking the course?

- How effective was the course in improving participants' cybersecurity knowledge and behaviors?

Outcomes and Contributions to the Body of Knowledge

The outcomes of this case study seek to provide insights into the effectiveness of the CS course in enhancing participants' preparedness in implementing cybersecurity practices. This research potentially contributes to the body of knowledge by assessing participants' initial perceptions and preparedness regarding cybersecurity practices through a pre-course survey and by evaluating the course's effectiveness via qualitative feedback from a post-course focus discussion. The findings highlight how the course influences participants' knowledge and preparedness in cybersecurity.

The findings of this study are not intended to be broadly generalized. However, the study does underscore the importance of blending technical, cybersecurity components, with human, psychological approaches in course design. The focus of this research is on how a well-structured and presented introductory cybersecurity course can improve knowledge and practical skills.

Structure of the Dissertation

Chapter 1, Introduction, establishes the objectives and significance of the study. It introduces the overarching research questions guiding the investigation and provides an outline of the dissertation's structure. This chapter sets the stage by explaining the study's context and rationale.

Chapter 2, Literature Review, reviews existing literature related to connectivism, cybersecurity education, and relevant theoretical frameworks. This chapter reviews previous

research findings, identifies gaps in the literature, and positions the current case study within the broader academic discourse.

Chapter 3, Methodology, details the methodology used in this study, including the research design, participant selection, data collection methods, and data analysis procedures. This chapter describes both the descriptive analysis and qualitative approaches employed to gather and analyze the case study data.

Chapter 4, Findings, presents the results of the descriptive analysis as well as the qualitative findings from thematic analysis of a focus group discussion. This chapter aims to present the data objectively to set the stage for discussion in the following chapter.

Chapter 5, Implications and Conclusions, interprets the case study findings presented in the previous chapter by discussing their implications for practice, theory, and policy. This chapter also offers recommendations for future research and explains the limitations of the study. It concludes by summarizing the contributions of the research to the field of cybersecurity education.

Delimitations

This study is a case study focused on individuals from the Texarkana region who enrolled in the CS course at Texarkana College. Participation was limited to those aged 18 years or older, without discrimination based on race, gender, or ethnic composition. The projected number of subjects was capped at 15 participants to allow for personalized instruction and the efficient use of limited lab computers.

Recruitment was conducted via an in-class announcement. The course is non-graded, and community orientated, potentially mitigating concerns of coercion or undue influence. Data collection involved an online pre-course survey administered via SurveyMonkey, taking

approximately 5-10 minutes to complete, and a post-course focus group session designed to last no longer than 30 minutes. This approach facilitated personalized feedback on the course's content, delivery, and overall effectiveness. This study only included participants who completed both the initial survey and subsequent focus group feedback. This delimitation ensured that the data collected was reflective of the participants' entire experience with the course.

Lastly, this study does not aim to generalize findings to all cybersecurity educational programs. Instead, by engaging in purposive sampling for a specific region, the insights gained are intended to provide context to how participants responded to introductory cybersecurity education.

Summary

Chapter 1 established a foundational understanding of cybersecurity, merging insights from NIST and Basie and Rossouw (2018) with historical developments like ARPANET and key incidents such as the LBL case. It highlighted the evolution of cybersecurity and the importance of protecting digital assets from internet threats. The chapter discussed different educational approaches to cybersecurity, using ODU's interdisciplinary course as a case study, and contrasted these methods with those used in community college settings. This paper aims to provide insights into the effectiveness of the CS course in enhancing participants' preparedness to implement cybersecurity practices.

Chapter 2 provides an examination of the current cybersecurity landscape that explores the increased risks of cybercrime, the financial impacts of cyber threats, and the importance of strong cybersecurity measures. It also discusses the role of education in preparing the next generation of cyber-resilient workers and examine the relevance of connectivism in cybersecurity education.

CHAPTER 2

LITERATURE REVIEW

Introduction

Threat Landscape

The evolving cyber threat landscape presents a challenge to organizations across various sectors. The potential risk of cybercriminals stealing information underscores the need for a comprehensive understanding of the institutional risks and effective countermeasures available to deploy. Microsoft, International Business Machines (IBM), and Sophos serve as a few of the critical gauges for understanding cybersecurity threats in depth, as they collectively underscore the urgency for resilient cybersecurity measures. Hogan-Burney (cited in Microsoft, 2023) notes that cybercrime is intensifying as criminals exploit human and technological vulnerabilities to stay ahead of security efforts. These adversaries exhibit a level of operational sophistication that mirrors legitimate business enterprises by constantly refining their tactics to circumvent improved security measures. They exploit business networks to conduct credential phishing campaigns, disseminate malware, and steal protected information from unwitting businesses for malicious gain (Microsoft, 2023). Longtchi et al. (2023) identified thirteen psychological techniques that attackers use to establish a level of trust with their potential victim:

- *Urgency*: Creates a sense of immediate action.
- *Attention grabbing*: Uses sensory stimuli to focus the victim's attention.
- *Visual deception*: Uses visual elements to induce trust.
- *Incentive and motivator*: Offers rewards to encourage compliance.
- *Persuasion*: Encourages certain behaviors by exploiting liking.
- *Quid-pro-quo*: Promises a high payoff in exchange for taking a risk.
- *Foot-in-the-door*: Gains compliance for a larger request by starting with smaller ones.

- *Trusted relationship*: Takes advantage of existing trust relationships.
- *Impersonation*: Assumes a false identity to increase compliance.
- *Contextualization*: Establishes commonality with the victim to increase attack success.
- *Pretexting*: Engages the victim by referring to relevant and current events.
- *Personalization*: Uses personal information to tailor messages and build trust.
- *Affection trust*: Establishes an affectionate relationship to make the victim more willing to take risks.

Had security hygiene practices such as enabling multifactor authentication (MFA) and establishing a zero-trust environment, initially been followed (see Figure 5 for cybersecurity hygiene principles), many of these attacks would have been reduced to merely unsuccessful attempts.

Figure 5

Cybersecurity Hygiene-In-Action



Threat Implications

IBM's *Cost of a Data Breach Report* (IBM, 2023) findings show that the financial

landscape of cybersecurity has been notably marked by an increase in the average total cost of data breaches, reaching a record high of USD 4.45 million in 2023. Phishing, a social engineering attack in which an attacker tricks the individual into revealing sensitive information, surpassed stolen or compromised credentials as the most frequent cause of data breaches, responsible for 16% of cases, while compromised credentials were involved in 15% of breaches (IBM, 2023). Phishing was not only the most frequent attack method utilized, but also the second most expensive cause with an average cost of USD 4.76 million (IBM, 2023).

Higher education emerged as the second most likely sector to experience ransomware, with a 79% likelihood. This ranking is just behind the lower education sector, which leads at 80%, a trend attributed to lower levels of technology resources (Sophos, 2023). Similarly, higher education institutions were most susceptible to attackers exploiting a vulnerability in the institution's system or user's credentials being compromised and accessed. The prompt application of software patches, continuous endpoint monitoring, and a regular review of security controls to ensure tools are functioning optimally can bolster cyber defenses and ward off common attacks (Sophos, 2023).

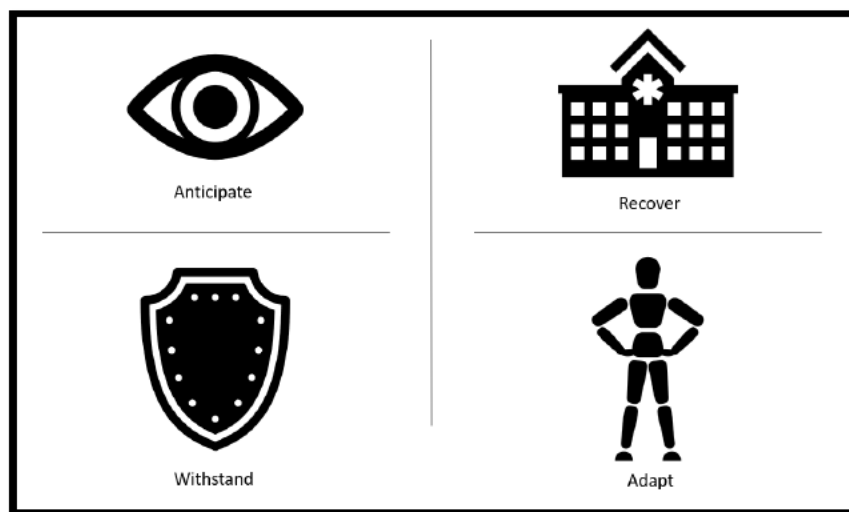
Expanding on cyber interactions among people, Lahcen et al. (2020) emphasize that the way people interact with software and technology, influenced by their biases and behaviors, plays a part in shaping the cybersecurity landscape. Enterprises should then design systems with the foresight of potential vulnerabilities, including human error, and prioritize avoiding vulnerabilities over patching them or allocating resources to defend against them (Lahcen et al., 2020). The authors further contend that the end user should be involved in the system design life cycle using simulation. This would allow the stakeholder to voice their opinions about operational characteristics prior to the production development phase.

Resiliency in Cybersecurity

The insights of Lahcen et al. (2020) regarding the impact of human behavior on cybersecurity suggest that an integrated approach to cybersecurity that encompasses the technological defenses, *and* the behavioral human elements is needed. Cyber resiliency, as defined by NIST, is the “ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources” (CSRC Content Editor, n.d.). The capacity to recover from or adapt to technological disruptions is the core function of a system designed to operate in critical situations (see Figure 6 for resiliency principles). Mailloux and Grimaila (2018) emphasize that strategically planning for, and effectively recovering from, various risk scenarios is crucial. This involves integrating cost-effective and reliable security and resilience features into the design process as a fundamental approach to addressing cybersecurity concerns.

Figure 6

Cyber Resilience Core Principles



Note. This figure depicts the four core principles of resiliency: anticipate, withstand, recover, and adapt. Each principle is symbolized by an icon representing the proactive and reactive measures essential for building resilience in various systems or situations.

The advancement of the cyber-resiliency field depends on the ability of cybersecurity experts to master and implement resiliency principles within secure systems. In a constantly evolving and vulnerable digital environment, cybersecurity experts must excel in crafting, refining, and confirming the security of systems, all while considering the immediate operational difficulties and interdependencies (Mailloux & Grimailla, 2018). Robust resiliency tactics are essential for counteracting both existing and emerging cyber dangers, covering all phases of a system's lifespan and confirming that security strategies are in harmony with business objectives and operational needs. Given the complexities of modern cyber-physical systems (CPS) and the ever-evolving threat landscape, there is a pressing need for education and training to equip the next generation of cybersecurity professionals with the necessary skills and knowledge. Microsoft's working pledge involves strong collaborations with schools, charitable groups, governmental bodies, and various companies in providing training tools that help individuals adjust to ever-changing difficulties (Microsoft, 2023).

National Cybersecurity Agenda

This commitment aligns closely with the objectives described in the recently released *National Cyber Workforce and Education Strategy*. The first pillar in this strategy emphasizes the need for all Americans to possess foundational cyber skills, a goal that resonates with Microsoft's initiative to enhance digital competencies across diverse sectors (Office of the National Cyber Director, 2023). This involves collaboration across academia, the public sector, and the private sector to deliver these opportunities effectively within their communities. Additionally, the agenda specifies that access to learning opportunities should be available to those interested, including affordable online environments (Office of the National Cyber Director, 2023). The key initiatives of this first important pillar are as follows:

- *Enhancing learning through federal support*: Leveraging federal investments to improve foundational cyber skill programs and ensure inclusivity through digital inclusion plans.
- *Ecosystem collaborations*: Encouraging content creation by industry experts and educators to foster a comprehensive approach to cyber skill education.
- *Open knowledge networks*: Promoting the development of a web-based open knowledge network for non-proprietary cyber skill resources.
- *Data-informed investments*: Using data to guide investment decisions in cyber skill education, including foundational cyber skills in existing educational frameworks.

Similarly, the National Initiative for Cybersecurity Education (NICE), in collaboration with NIST, has developed a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development (National Initiative for Cybersecurity Education, 2020). NICE aims to address the national shortage of cybersecurity professionals by increasing the size and capability of the global cybersecurity workforce and enabling the digital atmosphere to be responsive and agile to new conditions.

The second goal in the NICE strategic plan involves transforming education to develop and maintain a diverse and skilled cybersecurity workforce (National Initiative for Cybersecurity Education, 2020). Central to this transformation is the enhancement of educational practices that not only attract but also retain a diverse talent pool. The plan calls for the provision of critical skills that employers demand, while also advocating for a multidisciplinary approach to cybersecurity education. Lastly, section 2.6 of the strategy emphasizes the importance of promoting and valuing the contributions of educators, acknowledging them as a critical segment of the workforce in high demand (National Initiative for Cybersecurity Education, 2020).

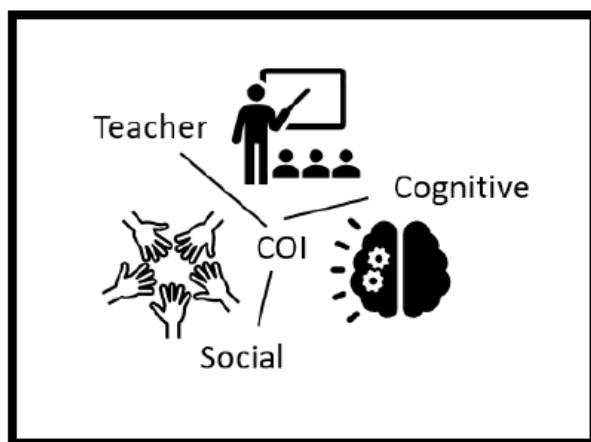
Cybersecurity and Curriculum Models

In line with the NICE (2020) emphasis on education, a comprehensive cybersecurity curriculum appears to be pivotal for arming students with the skills to protect digital assets and

maintain privacy in an increasingly interconnected world. Habrusiev et al. (2023) identified three pedagogical conditions that are part of modern higher education institutions: (1) a structured information and learning environment; (2) the training of students to operate the information and communication tools; and (3) the enhancement of information technology skills for modern information and computer technology-based teaching methods. The comprehensive exploration of digitalization's impact on education by Latorre-Medina and Tnibar-Harrus (2023) not only show the need for skilled professionals in digital learning environments, but also emphasizes the urgent requirement to incorporate robust digital security measures in teacher training programs. Their research, employing a combination of quantitative analysis and systematic reviews, uncovered a significant gap in the digital security preparedness of upcoming educators. This discovery points to the necessity for future teachers to receive more holistic and thorough instruction in cybersecurity, ensuring they are well-equipped to navigate and impart knowledge in the increasingly digitalized landscape of education.

Figure 7

Community of Inquiry (COI)



Nolan-Grant (2019) further establishes the crucial role of interactions between teachers and learners in online settings. This perspective aligns closely with the community of inquiry

(CoI) framework (Garrison et al., 2010), which includes social presence, teaching presence, and cognitive presence as its core elements (see Figure 7). While CoI has traditionally been utilized as a framework for investigating online learning contexts, this study argued that it can also serve as an effective model for designing online learning experiences.

A similar model, the universal design for learning (UDL, 2020) framework, encourages educators to apply multiple means of engagement, representation, and expression. The framework advocates for educators to proactively design curricula and teaching strategies that address a variety of student learning needs and preferences, rather than reacting to individual needs as they emerge (Sanger, 2020). This includes designing a variety of learning activities (e.g., visual aids, interactive tools, informal and formal discussions, reflective writing) so that students with different learning abilities feel included.

Agile Strategies in Curriculum Design

Owen and Wasiuk (2021) explored the use of agile methodologies in higher education by focusing on a collaborative partnership with students. The researchers designed their partnership around the concept of micro-sprints (short, iterative cycles in which collaboration, feedback, and adjustments were done with diverse student volunteers) in which a team would plan, build, review, and retrospect on their current goal. Weekly reflections were gathered to continuously enhance the process and fine-tune the approach within a secure, cooperative setting. These reflections guided the sprint actions, which were intended to facilitate incremental and beneficial modifications to the sprint procedure (Owen & Wasiuk, 2021). Similarly, and to create a more consistent and interdisciplinary learning experience for students, Woszczyński et al. (2021) collaborated with faculty members from different universities in applying agile methodologies to course development. Termed the Agile Collaboratively Developed Course (ACDC), the

researchers' agenda was to assess course materials for an Information Systems (IS) course and determine whether those materials were consistent across course sections. The study found that teams applying the ACDC methodology in curriculum design tend to achieve higher engagement and increased interaction, both in virtual classrooms and among a diverse group of professors and universities (Woszczynski et al., 2021).

In cybersecurity education specifically, Workman et al. (2022) explored the gap between the abundant availability of educational material and the practical application of cybersecurity principles. The study leveraged the present-test-practice-assess (PTPA) model, which emphasizes a focused presentation of materials, immediate conceptual testing, practical application through practice, and subsequent performance evaluation. The findings suggest that cybersecurity simulations, as compared to traditional training methods, can enhance learning performance. The article further emphasizes the necessity of shifting from merely disseminating information to instigating behavioral change in cybersecurity practices.

One of the methods in which cybersecurity education has been taught, and further emphasizing the findings by Workman et al. (2022), is through digital games. Ros et al. (2020) designed a game to introduce basic cybersecurity concepts. Structured using the constructivism learning theory that proposes “we construct our perspective of worlds through individual experiences and schema” (p. 97720), the researchers examined the impact of two variables (engagement and context) on students' perceptions of their learning success. An interesting insight from the authors centered on the increased dropout rates among students who opted out of playing the game, implying that the decision to not participate in the game might be an early sign of potential dropout (Ros et al., 2020). The comprehensive analysis of 181 cybersecurity games by Coenraad et al. (2020) highlights the importance of making game-based cybersecurity

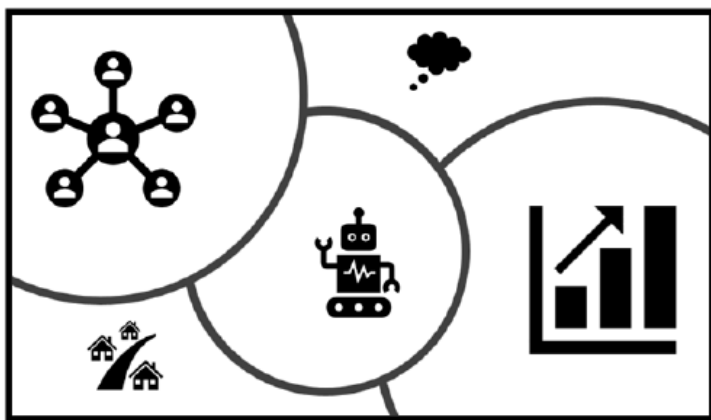
content more accessible and available in diverse locations. Additionally, the authors suggest that incorporating social elements into future game designs could provide a more well-rounded perspective on cybersecurity.

Social Cybersecurity

Concerning social elements, Carley (2020) focused on building a resilient cyber infrastructure in the field of social cybersecurity (see Figure 8). The author noted that while traditional cybersecurity experts are typically versed in technology, computer science, and engineering, those specializing in social cybersecurity should have expertise in social communication, community building, statistics, social networks, and machine learning (2020). Researchers from various disciplines were instrumental in developing this social science. Consequently, the National Academies of Science (NAS, 2019) set forth two main goals: to identify how cyber-mediated factors alter behaviors and outcomes at various levels, and to aid in constructing the necessary cyber infrastructure to protect against cyber-mediated threats (Carley, 2020).

Figure 8

Social Cybersecurity



Note. The components of social cybersecurity are depicted in Figure 8, highlighting the interaction between community networks, autonomous AI, and analytics for improved security measures.

Theoretical Framework

Connectivism

Digital transformation is significantly influencing the educational environment, with traditional modes of communication giving way to virtual interactions, as explored by Baeva (2021) in the context of digital learning systems. This educational evolution closely aligns with the emerging needs in cybersecurity education for interdisciplinary approaches, improved digital skills, thorough course design, and societal integration, all which align well with the principles of connectivism. Connectivism was first introduced as a response to the educational challenges and opportunities due to the digital revolution (Siemens, 2005). This theory suggests that learning transpires through the navigation and connection within information networks, a process facilitated by digital literacy and the critical evaluation of information (Siemens, 2005). It underscores the necessity for learners to adeptly manage information and foster lifelong learning skills while adapting to the ever-changing digital landscape. Siemens identifies the principles of connectivism as:

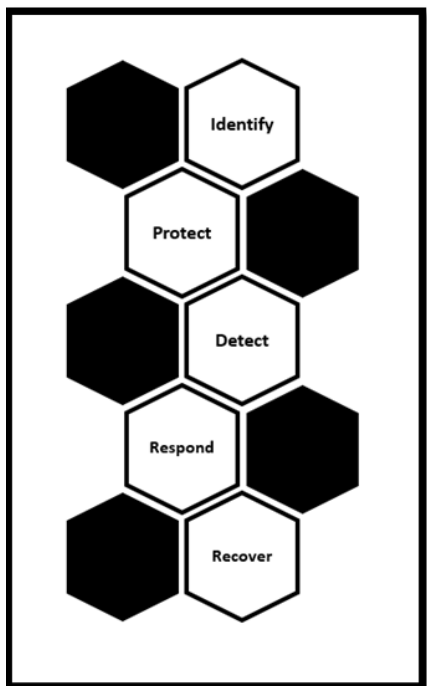
- Learning and knowledge rest in diversity of opinions.
- Learning is a process of connecting specialized nodes or information sources.
- Learning may reside in non-human appliances.
- Capacity to know more is more critical than what is currently known.
- Nurturing and maintaining connections are needed to facilitate continual learning.
- The ability to see connections between fields, ideas, and concepts is a core skill.
- Currency (accurate, up-to-date knowledge) is the intent of all connectivist learning activities.
- Decision-making is itself a learning process. Choosing what to learn and the meaning of incoming information is seen through the lens of a shifting reality. While there is a right answer now, it may be wrong tomorrow due to alterations in the information climate affecting the decision.

Connectivism Examined

In examining connectivism, Goldie (2016) remarked that the initiation of learning takes place when learners engage with and become part of a learning community (which are nodes within the connectivist model). These nodes take the form of websites, organizations, databases, journals, libraries, social media, peers, blogs, discussion boards, YouTube videos, podcasts, OER, professional associations, and other specialized lighthouses that are networked to share resources. Stephen Downes (2006), expander of connective knowledge, suggests that learning and knowledge are not solely about the content but about understanding the relationships and networks that link various pieces of information together. Perspective and ideas that were previously not considered, due to sporadic network connections or lack of a community, are able to structure their views via the technology of their choosing and present it among community members.

Figure 9

Framework Functions



As a result, a stable connection is formed that, when nurtured and addressed, can develop into information highways in which stored and accessible knowledge is shared among the community. However, as information shifts in and out of relevance, the skill to search for up-to-date information and discern between secondary and non-essential information is regarded as a crucial ability that enhances the learning process (Goldie, 2016). This ability is like the core functions described in *The Framework for Improving Critical Infrastructure Cybersecurity* (NIST, 2018). Labeled as *identify, protect, detect, respond, and recover* (see Figure 9), these functions are meant to provide an organization with a strategy for addressing the dynamic nature of cybersecurity and the inherent risks associated with technology. The functions of this framework will serve as the basis for the WECM learning outcome of applying NIST standards and best practices.

Connectivism and NIST

In connectivism, the goal of all learning activities is to achieve currency (accurate and current knowledge) (Siemens, 2005). This aligns with the leaning outcome in that both practice and theory emphasize the importance of remaining current with information as technologies are habitually shifting. The learner is acquiring the knowledge and understanding to apply NIST guidelines, while evaluating and updating their current connections to ensure the information is relevant and applicable. Given the ongoing risk posed by malicious actors exploiting zero-day vulnerabilities and targeting end users, (Whisenant, 2022), it is crucial to persist in researching and enhancing our digital maturity and environment. In adopting cybersecurity guidelines, the first function in the NIST framework (identify) is potentially satisfied.

Recent Studies

Critical Infrastructure Security

The Security and Privacy Controls for Information Systems and Organizations is a joint task force effort in developing information security standards and guidelines for federal information systems (NIST, 2020). Notably, Section 3.6 addresses contingency planning, stressing the necessity of a robust disaster recovery (DR) plan. This aligns with the recover function of the NIST core functions framework in emphasizing preparedness for system breaches and restoration. This alignment underscores the importance of developing backup and recovery procedures as a key learning outcome for cybersecurity education. According to the Center for Internet Security (CIS), the purpose of a contingency planning policy is to ensure the availability of normal IT resources during unforeseen circumstances (CIS, n.d.). As connectivism emphasizes the value in diversity of thought, learners can explore the different perspectives and strategies related to backup/recovery procedures while collaboratively designing a DR manual. This process potentially enriches their understanding of the practical application of cybersecurity education while also satisfying the LO of contingency planning.

In association with Siemens' (2005) principle that learning potentially exists outside of the human model, the role of artificial intelligence (AI), automation, and interactive feedback are crucial components in cybersecurity education. By engaging with digital platforms and AI-driven tools, students are not only exposed to the latest technological advancements but also develop a deeper understanding of emerging vulnerabilities associated with these technologies. To best protect from emerging vulnerabilities, students' understanding of various operating systems' security features provides a foundation to begin applying a layer of safety around system data. connectivism's approach encourages students to tap into the collective intelligence of their peers through online communities thus adding to their educational experience. By using lighthouses and forming stable connections with the larger cybersecurity community, the LO of using

desktop/device operating system features to implement security is potentially satisfied.

The protect function in the NIST cybersecurity framework plays a crucial role in maintaining the security and integrity of systems. Through this function, the following safeguards are enacted that potentially quarantine a cybersecurity incident while ensuring critical systems remain uninterrupted:

- *Implementation of data security measures:* This involves establishing robust data security protocols aligned with the organization's risk strategy. Such measures are crucial for safeguarding the confidentiality, integrity, and availability of information, as per NIST (2023) guidelines. Tactics include deploying encryption techniques, setting appropriate access controls, and employing other strategies to secure data.

- *Management of protective technologies:* This process is centered on ensuring that the security and resilience of systems follow the organization's established policies and procedures (NIST, 2023). The strategic deployment and management of technologies like firewalls, antimalware applications, and other protective measures, are fundamental to ensuring digital safekeeping.

In comparing the protective safeguards with the connectivist idea of recognizing the value among disciplines, we see a connection form in that both the principle and the safeguards emphasize identifying areas in which information needs to relate to the applicable node. This perspective fosters an environment where learners are encouraged to draw connections between diverse fields such as security policies, threat intelligence, and vulnerability assessments. By integrating knowledge from these various domains, learners are equipped to develop comprehensive strategies for mitigating cybersecurity threats. If successful, this will fulfill the learning outcome of being able to identify computer and network threats and vulnerabilities, as

well as the methods to prevent their effects.

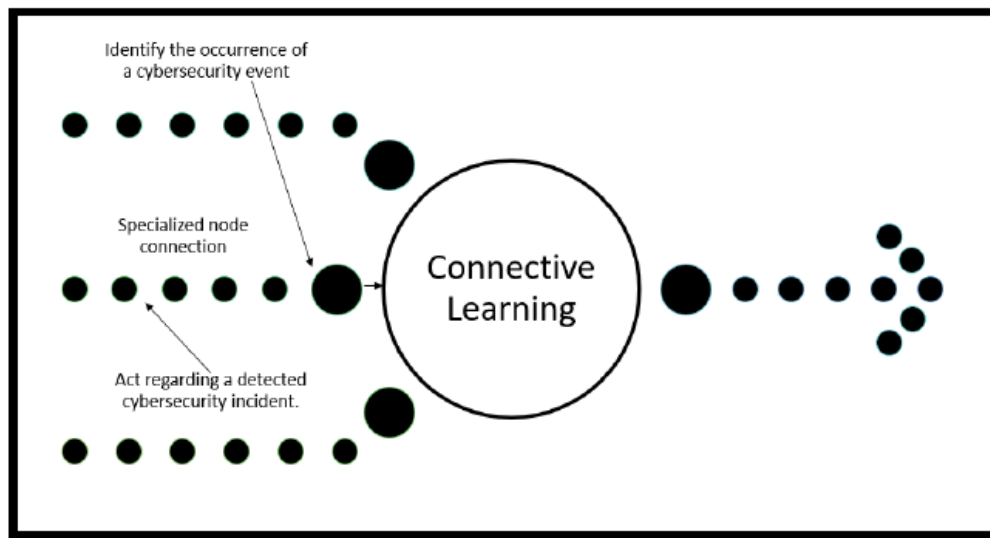
Connective Learning

For consolidation purposes, the final two LOs will be combined as their similarities lead to a merging of their goals. Respectively, the principles of connectivism will be consolidated, focusing on the ideas that learning involves connecting specialized nodes or sources of information, and that the ability to acquire new knowledge is more vital than the knowledge currently possessed, as outlined by Siemens (2005). In combining the LOs, the ability to use tools and encryption techniques to enhance network and data security, will now serve as the new standard in accessing how students use cybersecurity toolkits, connect with professional members of the learning community, and conduct research to ensure current information is being processed among the members. This approach also aligns with the NIST functions of detect and respond (NIST, 2018).

Siemens (2005) emphasizes the importance of establishing nodes for networking and sharing of information. When nodes, or lighthouses in our study, form connections with other nodes, dynamic and diverse pathways emerge that potentially leads to collaborative learning. If developed and stabilized, the learner is better positioned to navigate an evolving information landscape. Lifelong learning potentially emerges because of these principles, thus allowing the learner to stay connected, informed, and relevant in the learning community (see Figure 10). By combining both principles and the established learning objective, simulated ransomware scenarios emerge as a potential activity for disseminating informational techniques on specific security tools or various techniques for thwarting threat actors. Simulated information security incidents could be reflected upon thus leading to collective analytical experience in which ideas are shared and critiqued.

Figure 10

Connectivism and Cybersecurity



Note. This figure merges the concept of connectivism with cybersecurity. The dynamic network of learning is illustrated where nodes represent the acquisition and application of knowledge in detecting and responding to cybersecurity events.

Evidentiary Information

Alsaleh (2020) explains that the role of the instructional designer is to identify the issue, determine the existing gap in needs, and pinpoint its causes along with potential solutions. In the context of our study, this observation forms the basis of our needs assessment. The evolution of the threat landscape, as described in reports by Microsoft, IBM, and Sophos, necessitates an educational understanding of tactics such as credential phishing, malware dissemination, and the exploitation of human and technological vulnerabilities. This evolution underscores the need for continuous education and training to keep up with these rapidly changing threats. Moreover, the literature review emphasizes the importance of security hygiene practices, such as MFA, highlighting a significant gap in basic cybersecurity principles and practices education, which can prevent many common attacks when properly taught and implemented (Microsoft Copilot, 2023).

From a financial perspective, IBM has shown the costly implications of data breaches, stressing the need for integrating security principles into the development process to mitigate these risks. In terms of education, training programs are critical in preparing the next generation of cybersecurity professionals to prevent costly security failures. The focus on resilience in the tech sector emphasizes the importance of education that prepares for, endures, and rebounds from cyber incidents. This includes creating systems with inherent robustness and equipping professionals to strategically approach long-term cybersecurity.

Additionally, the use of psychological tactics in social engineering attacks indicates the necessity for a comprehensive approach that combines both technological and behavioral aspects of cybersecurity. Lastly, the focus on accessibility in the National Cyber Workforce, alongside NICE's goal of developing a diverse and skilled workforce, underscores the necessity for inclusive and accessible cybersecurity education.

Summary

Chapter 2 provided an examination of the cybersecurity landscape, the risks posed by cybercrime, and the need for robust cybersecurity measures. The insights from corporations like Microsoft, IBM, and Sophos stress the financial impacts of cyber threats, and the importance of strong cyber defenses in maintaining resiliency. Additionally, the chapter discussed the psychological tactics used in cybercrime, the significance of human factors in cybersecurity, and the need for foundational cyber skills.

Chapter 3 details the study's methodology. This includes the mixed-methods approach used to evaluate initial cybersecurity awareness among community members, and the thematic analysis process used in detailing the participant feedback.

CHAPTER 3

METHODOLOGY

Introduction

This case study adopted a mixed methods design to explore the effects of an introductory cybersecurity education course on residents in northeast Texas. Quantitative data from a pre-course survey is descriptively analyzed and qualitative feedback from a focus group discussion is thematically analyzed to provide insights into the participants' cybersecurity knowledge after attending the course. While the initial survey included questions regarding participants' familiarity and engagement with connectivism, the focus of this case study is specifically on the effects of an introductory cybersecurity education course.

The study also assessed the initial perceptions and preparedness of participants regarding their cybersecurity practices before participating in the course. In reviewing the qualitative feedback, the study also evaluated participants' perceptions of the course's effectiveness and benefits in enhancing their understanding of cybersecurity.

Based on these findings, recommendations for improving the CS course were provided. While the insights gained were valuable, they are specific to the case study and meant as guidance, rather than definitive conclusions, for similar institutions.

Study Goals

This study had several objectives that focused on understanding the impact of the CS course on participants in northeast Texas, specifically in the Texarkana area. The pre-course survey helped establish participants' knowledge and readiness levels regarding their cybersecurity practices. Additionally, the qualitative feedback helped to understand the course's effectiveness in enhancing their understanding of cybersecurity education. Though specific to

this case study, these findings provided perspectives on how the course influenced participants' learning experiences and their perceived ability to apply cybersecurity practices.

Research Questions

The research questions in this study are designed to explore participants initial perceptions and outcomes from the CS course. These questions are important for assessing initial participant views on cybersecurity practices and how the course improved their knowledge and preparedness. The case study is guided by the following research questions:

1. What were participants' perceptions of cybersecurity practices before taking the course?
2. How effective was the course in improving participants' cybersecurity knowledge and behaviors?

Research Design

The research design for this case study adopted a mixed methods approach, incorporating both quantitative and qualitative data to evaluate the CS course. This approach allowed for descriptive analysis of the participants' initial knowledge and readiness, as well as their perceptions of the course's effectiveness.

Quantitative Component

The quantitative component of the study involved a pre-course survey to assess participants' baseline understanding and preparedness regarding cybersecurity practices. The survey gathered data on participants' beliefs about the importance of cybersecurity, confidence in identifying and protecting against cybersecurity threats, proactive behaviors in seeking out cybersecurity information, and the prioritization of basic cybersecurity practices. Additionally, demographic information, such as age, education level, and work/study area, were also collected

to explore potential influences on participants' initial knowledge and preparedness.

Qualitative Component

The qualitative component consisted of post-course focus group discussion questions to gather feedback on participants' experiences and perceptions of the course. This approach allowed for an exploration on how the course impacted participants' understanding of cybersecurity practices. Participants' feedback were coded and analyzed to identify recurring themes and insights related to their satisfaction and perceived improvements.

Setting

Institutional Review Board (IRB) approvals were obtained from both the University of North Texas (UNT), the host institution for this research, and Texarkana College (TC), the community college where the study was based (see Appendix A). The study was conducted within the context of the CS course offered at TC.

Participants

Sampling Procedure

A purposive sampling method was employed to select participants who were actively engaged in the CS course and could provide relevant insights into their learning experiences. The sample size for this study was determined based on course enrollment, in which a total of 15 participants completed the pre-course survey to assess their knowledge and preparedness in cybersecurity practices. Following the course, eight participants participated in a focus group discussion and shared their insights and perceptions of the course. The insights gathered contribute valuable information to the case study and are considered within the context of the study.

Target Population

The target population for this study consisted of community members enrolled in the CS course at TC. The diverse demographic composition of Texarkana, which spans both Texas and Arkansas, provided a rich context for the study by capturing a wide range of age groups, educational backgrounds, and technology access levels. Approximately 17.2% of the population in Texarkana, Texas, is over 65 years old, and 59.1% are between the ages of 18-64, with similar age distributions in Texarkana, Arkansas. Educational attainment levels are also varied. In Texarkana, Texas, 89.3% of residents aged twenty-five and over have at least a high school diploma, and 23.3% hold a bachelor's degree or higher. In Texarkana, Arkansas, 87.4% have high school diplomas or higher, and 16.1% have attained a bachelor's degree or higher. Regarding technology access, 80.9% of households in Texarkana, Texas, and 90.2% in Arkansas have a computer. In Texarkana, Texas, 74.6% of households have broadband internet subscriptions, while on the Arkansas side it is slightly higher at 80.1%, indicating a disparity in digital access that may have affected interactions with cybersecurity course content (U.S. Census Bureau, 2022).

Recruiting Approach

The recruitment approach for this study was designed to ensure the voluntary and informed participation of community members enrolled in the CS course. The process began with the distribution of a recruitment flyer approved by UNT (see Appendix B). The flyer provided an overview of the study, including its purpose, procedures, and the benefits of participation. Each potential participant received a paper informed consent form (see Appendix C) outlining the study's purpose, procedures, risks, and assurances of confidentiality. The consent form emphasized the voluntary nature of participation and assured individuals of their

right to withdraw from the study at any time without any repercussions.

Data Collection

This section describes the instruments used in the study to collect data. Two primary instruments were employed: the pre-course survey (see Appendix D) and the focus group discussion questions (see Appendix E).

Pre-Course Survey

The pre-course survey, administered online using SurveyMonkey, assessed participants' initial knowledge and preparedness regarding their cybersecurity practices before engaging with the CS course. The survey included questions concerning participants' belief about the importance of cybersecurity, confidence in identifying and protecting against cybersecurity threats, proactive behaviors in seeking out cybersecurity information, and the prioritization of basic cybersecurity practices. Additionally, the survey collected demographic information such as age, education level, and work/study area to descriptively analyze potential influences on participants' initial knowledge and preparedness.

Focus Group Discussion Questions

At the conclusion of the CS course, participants were invited to participate in a focus group discussion to provide feedback on their experiences and perceptions of the course. The focus group discussion questions were designed to elicit responses about the course's content, delivery, and overall effectiveness. The questions aimed to gather insights into participants' preparedness in implementing cybersecurity practices after completing the course.

Data Analysis

Data Preparation

Prior to analysis, all survey responses were reviewed for completeness and no issues or outliers were found. The survey results were analyzed descriptively to present the initial perceptions and preparedness of the participants. The focus group discussion responses were transcribed electronically for thematic analysis.

Quantitative Analysis Procedures

The demographic data, including participants' age group, education level, and work or study area, were analyzed using descriptive statistics to provide a clear overview of the participant population. Categorical data such as age group and education level were reported in terms of frequencies and percentages. For the Likert-scale questions related to participants' self-evaluation of cybersecurity knowledge and practices, descriptive measures, including the mean (M) and standard deviation (SD), were calculated. No further inferential analyses were conducted because the study was limited to a single group of participants and no comparisons or follow-up data were collected.

Qualitative Analysis Procedures

The qualitative data collection process involved gathering feedback from participants who completed the CS course through a post-course semi-structured focus group discussion. The objective was to gain insights into participants' experiences, perceptions, and suggestions regarding the course. The qualitative data complemented the quantitative findings and provided a broader understanding of the course's impact on participants.

Transcription and Coding Process

To ensure all responses were accurately captured, the feedback from the focus group discussions was directly transcribed into a digital format during the sessions. Once the data was

transcribed, thematic analysis, as outlined by Braun and Clarke (2006), was employed to identify patterns within the data. The analysis began with an initial reading of the transcribed data multiple times to become familiar with the content and to identify recurring ideas for coding. Initial codes were generated based on repeated words and phrases observed in the feedback, such as ‘engaging content’ or ‘user experience.’

Categorization and Theme Identification

The initial codes were reviewed and refined to ensure they accurately reflected the data. Redundant or overlapping codes were combined, resulting in a set of codes that captured the key aspects of the participants’ feedback. These codes were then grouped into broader topics, which were further analyzed to identify overarching themes that represented the main points of feedback.

Validation Procedures

During the focus group discussion, follow-up questions were used to clarify participants’ responses in real time. Additionally, peer debriefing involved discussing the research process with experienced colleagues, as their feedback helped ensure an appropriate case study was implemented.

Threats to Validity

Potential threats to validity, such as researcher bias, were acknowledged and addressed:

- *Researcher bias*: Reflexivity, as defined by Heaton (2004), “generally involves the self-examination of how research findings were produced, and, particularly, the role of the researcher in their construction” (p. 104). This approach was employed throughout the research process to remain aware of potential biases and how they might affect data interpretation.

- *Sampling bias*: Participants in the CS course were asked to participate in the study.

As a result, the sample reflects those who joined the course.

- *External validity*: The focus on a particular course and group of participants means that the findings are context-specific and may not be easily generalized to other settings. While the study provides valuable insights, they should be understood within the case study and not generalized to a broad population.

Summary

Chapter 3 outlined the research methodology used to assess the impact of the CS course on participants' cybersecurity knowledge and practices. The mixed-methods design process employed both descriptive analysis and qualitative feedback for this case study. Additionally, the chapter outlined the setting, participant demographics, sampling and recruiting procedures, data collection instruments, data preparation and analysis procedures, and validation measures.

Chapter 4 presents the results of the analysis, including descriptive statistics from the quantitative data and thematic analysis from the qualitative feedback.

CHAPTER 4

FINDINGS

Introduction

The purpose of this chapter is to present the findings from the data analysis to address the research questions outlined in this case study. The analyses include descriptive statistics and thematic analysis with the goal of evaluating participants' initial understanding and preparedness regarding cybersecurity practices, and the impact of the CS course.

The quantitative results are presented first. This analysis provides an overview of participants' demographic information, self-reported cybersecurity knowledge, and their current cybersecurity practices. These results are followed by the qualitative findings from the post-course focus group discussion, where participants' experiences with the course and its perceived impact on their cybersecurity preparedness are explored.

Quantitative Results: Research Question 1

Overview of the Research Question

To assess participants' initial knowledge and attitudes towards cybersecurity, a quantitative survey was administered to participants prior to the course. The survey responses potentially offer insight into how participants perceived the importance of cybersecurity, their confidence in identifying and addressing threats, and the basic practices they considered important in their digital life. These initial findings provide an important understanding of the participants' cybersecurity awareness and preparedness.

Demographic Data

The demographic data collected from participants helps to frame the study's findings by outlining their backgrounds (see Table 1). In terms of age, the majority of participants fell within

the 35-44 age range, representing 40% of the group (six participants). This was followed by 33.33% (five participants) who were between 25-34 years old. The 45-54 age group made up 13.33% (two participants), and both the 55-64 and 65+ age groups accounted for 6.66% each (one participant in each category). This suggests that most participants were middle-aged adults, with a few from both younger and older age groups.

Table 1

Demographic Data

Participant	Age Group	Highest Level of Education Completed	Work or Study Area
1	25-34	Some college	Healthcare
2	25-34	Associate degree	Healthcare
3	25-34	Associate degree	Information Technology
4	25-34	Bachelor's degree	Business
5	25-34	Bachelor's degree	Healthcare
6	35-44	Bachelor's degree	Business
7	35-44	Associate degree	Other (Trade)
8	35-44	Bachelor's degree	Other (Program Professional)
9	35-44	Master's degree	Healthcare
10	35-44	High school or equivalent	Healthcare
11	35-44	Associate degree	Healthcare
12	45-54	Master's degree	Healthcare
13	45-54	Bachelor's degree	Healthcare
14	55-64	Associate degree	Business
15	65+	Some college	Business

In terms of education, participants had varied academic backgrounds. One-third of the participants (33.33%, or five participants) had bachelor's degrees, while another 33.33% (five participants) held associate degrees. Participants with master's degrees made up 13.33% of the group (two participants), as did those who had completed some college but did not hold a degree (13.33%, or two participants). Only one person (6.66%) reported high school or equivalent as

their highest level of education. Overall, the participants tended to have higher education levels, with most holding formal degrees.

Regarding their occupation, more than half of the participants (53.33%, or eight participants) worked in healthcare, making it the largest field in this study. Those who work in business accounted for 26.66% (four participants), while information technology represented 6.66% (one participant). Two participants (13.33%) selected “Other” as their field, citing roles in trade and program management.

Survey Data

The Likert scale data (see Table 2) collected from the participants provided perspectives into their beliefs and behaviors concerning cybersecurity before taking the CS course.

Participants showed a strong belief in the importance of understanding cybersecurity, with an average score falling between agree and strongly agree ($M = 4.53$, $SD = 0.62$), indicating a consistent agreement across respondents. Confidence in identifying and protecting against cybersecurity threats, however, was lower, with most participants reporting ‘not so confident’ to ‘somewhat confident’ levels ($M = 2.4$, $SD = 0.80$), demonstrating more variability in responses. When it comes to proactive behaviors, such as actively seeking out information about cybersecurity threats, participants showed moderate levels of engagement, with responses averaging between ‘neither agree nor disagree’ and ‘agree’ ($M = 3.13$, $SD = 0.81$). This reflects some variability in how participants actively seek to stay informed.

Regarding the categorical question in which participants were asked to select a basic cybersecurity practice they deem most important (see Table 3), the results show that using strong passwords and enabling two-factor authentication were the most frequently selected practices, each chosen by five participants (33.33%). This indicates that two-thirds of the participants

prioritize these two access control measures in their digital security practices. Fewer participants selected using antivirus software and regularly updating software, with two participants (13.33%) choosing each option. Only one participant (6.66%) identified avoiding public Wi-Fi for sensitive transactions as the most important practice. These results suggest that participants place greater emphasis on access-related security practices, while other protective measures, such as antivirus software and secure connection practices, are considered less critical.

Table 2

Likert Scale Data

Belief/Behavior	M	SD	Response Summary
Importance of understanding cybersecurity	4.53	0.62	Responses averaged between 'Agree' and 'Strongly Agree'
Confidence in identifying and protecting against threats	2.40	0.80	Responses ranged from 'Not so confident' to 'Somewhat confident'
Proactive behaviors (seeking information on cybersecurity)	3.13	0.81	Responses averaged between 'Neither agree nor disagree' and 'Agree'

Table 3

Categorical Data

Cybersecurity Practice	Freq	%
Using strong passwords	5	33.33
Enabling two-factor authentication	5	33.33
Using antivirus software	2	13.33
Regularly updating software	2	13.33
Avoiding public Wi-Fi for sensitive transactions	1	6.66

Qualitative Results: Research Question 2

Overview of the Research Question

This section addresses the effectiveness of the course in improving participants' knowledge and behaviors related to cybersecurity. A thematic analysis of participants' feedback

revealed insights into how the course enhanced their understanding and ability to implement cybersecurity practices. The analysis focused on identifying key themes that reflect participants' perceptions of how the course influenced their preparedness and behavioral changes in cybersecurity.

Thematic Analysis Process

The thematic analysis for this case study was conducted to effectively organize and interpret the participants' feedback from the focus group discussion. The process followed several structured phases to ensure a complete understanding of the key themes related to the course's effectiveness, while following the framework outlined by Braun and Clarke (2006).

The following steps were taken to ensure a thorough analysis of the data:

- *Familiarization with the data:* The first step involved reviewing the digital transcript from the focus group to understand participants' feedback and perspectives. To maintain objectivity, one reviewer with expertise in cybersecurity was also asked to evaluate the feedback.
- *Generating initial codes:* Codes were generated by identifying recurring words, phrases, and ideas that appeared in the participants' feedback. The coding was conducted by a single coder, with a second coder (expert in cybersecurity) reviewing the initial analysis for accuracy and objectivity.
- *Searching for themes:* The codes were then organized into potential themes by grouping similar codes to potentially identify broader patterns.
- *Reviewing themes:* The themes were reviewed to ensure they accurately represented the coded data and were coherent across the entire dataset.
- *Defining and naming themes:* Each theme was refined and named to ensure it reflected the data and was distinct.

- *Producing the report:* The final step involved summarizing the themes with supporting quotes from participants to show the key findings.

Analysis of Emergent Themes

Each theme with related participant comments is examined below. Themes are organized under broader topics that correspond to the research questions.

Overall Impressions

Participants praised the course for being both engaging and informative, with one remarking, “The course was very engaging and informative,” while another noted, “The training was good, and the quality of the site was very well designed.” The inclusion of interactive elements and video content was especially valued, as this, “...broke up the monotony of reading and scrolling,” reflecting how these features contributed to a better user experience. The course’s user-friendly structure was noted by participants, with one stating, “There is a tremendous amount of information here. It’s laid out well and easy to navigate even for a novice like me,” emphasizing the accessibility of the material for individuals with different levels of technical expertise. Another added, “I liked how the course was set up and designed,” pointing to the well-organized presentation of the content.

Participants also appreciated the relevance and up-to-date nature of the material, particularly the “evolving ecosystem of learning that responds to and reacts to student feedback, keeping the content fresh.” They also noted the ease of access and understanding, describing the website as being “laid out very well” and easy to navigate. This emphasis on structure and accessibility was crucial in delivering an effective and meaningful learning experience.

Table 4

Overall Impressions

Theme	Defining Characteristics	Examples
Interesting and Informative	Captures participants' attention and provides valuable content	• “Very interesting and informative.” • “The training was good, and the quality of the site was very well designed.” • “The content, design and user experience are unbelievable.”
Well-designed and User-friendly	Features a well-thought-out layout and user experience; easy to navigate	• “I liked how the course was set up and designed.” • “There is a tremendous amount of information here. It’s laid out well and easy to navigate even for a novice like me.”
Engaging and Interactive	Keeps participants actively involved and provides a pleasant experience	• “The course was very engaging and informative.” • “I found the entire user experience to be intuitive, interactive, pleasant, informative, and fascinating.” • “Finally, I enjoyed the video content throughout the design. It broke up the monotony of reading and scrolling.”
Relevant and Up to date	Incorporates evolving, relevant content	“I especially enjoyed the concept of an evolving echo system of learning that responds to and reacts to student feedback, keeping the content fresh.”
Accessible and Understandable	Content is easy to access and understand	• “Wow to your website! The information is laid out very well. I was able to navigate through it easily.” • “I found the content easy to access and understand.”

Presentation and Engagement

Participants were generally appreciative of the presentation and engagement aspects of the course, frequently commending the instructor’s preparedness and clarity. “I could tell you had prepared well...your presentation was good, and you were confident in the presentation,” potentially reinforcing the value of a well-structured and professionally delivered curriculum. As such, the curriculum was seen as engaging and effective, “particularly in how it reinforced key

cybersecurity concepts.” and “...allowed me to explore subjects covered in greater depth,” demonstrating that the interactive elements supported a more thorough understanding of the material.

Table 5

Presentation and Engagement

Theme	Defining Characteristics	Examples
Well-prepared and Confident	Demonstrates thorough preparation and confidence in delivery	• “I could tell you had prepared well...your presentation was good, and you were confident in the presentation.” • “Great job!”
Effective and Engaging	Keeps participants actively involved and reinforces the curriculum’s benefits	• “The curriculum was very effective, particularly in the way it re-reinforces the benefits of participating in various online communities.” • “I found the most engaging portion of the course to be the CS-GPT, as it allowed me to delve deeper into the subjects covered in the course at my own discretion.”
Balanced Content	Integrates Connectivism and cybersecurity information	“The balance between connectivism (engaging in various networks / Lighthouses) and incorporating the information provided by NIST helps with understanding and implementing cybersecurity practices.”
Need for Interactivity	Desire for more hands-on exercises and interactive elements	• “The only area I can think of to critique would be the lack of any hands-on exercise. I find that I retain information better when I’m able to interact with the material.” • “I feel like more interaction could help lock in the knowledge provided. As a user that attended the Zoom meetings, it’s possible that I missed out on some of these activities, if they were present.”
Usability Issues	Minor usability problems such as font color contrast	“My only small constructive thought in terms of usability and function is a few places where the font color was difficult to see while reading.”

However, despite the positive feedback on the interactive elements, participants expressed a need for more hands-on exercises, emphasizing that they “retain information better”

through interaction with the material and that “more interaction could help lock in the knowledge provided.” These remarks emphasize the need to balance instruction with real-world applications, as doing so can potentially improve both retention and engagement.

Understanding and Application

Participant feedback revealed a clearer understanding of cybersecurity threats and ways to mitigate them, with participants reporting “a better understanding of what threats exist and what can be done to prevent those threats.” They also expressed intentions to apply the knowledge gained by planning to use “MFA, a password manager,” and keep their devices “up to date with the latest security patches.” This feedback demonstrates the course’s role in encouraging participants to take proactive steps in enhancing their cybersecurity practices.

Table 6

Understanding and Application

Theme	Defining Characteristics	Examples
Improved Understanding	Better knowledge of cybersecurity threats	“From participating in this course, I have a better understanding of what threats exist, and what can be done to prevent those threats from impacting me.”
Practical Application	Implementation of learned cybersecurity practices	• “I’ll be using MFA, a password manager, and try to keep my devices up to date with the latest security patches.” • “I have a better understanding of the fundamentals of cybersecurity.”

Usability and Navigation

Participants provided consistent positive feedback regarding the course’s usability and navigation, praising it as “very well designed” and describing the information as “laid out well and easy to navigate even for a novice.” The video content was appreciated for being approachable, as the videos “weren’t overly intimidating” due to their manageable length. The

course's user-friendly design was further emphasized by feedback that described the user experience as "intuitive, interactive, pleasant, informative, and fascinating." This feedback demonstrates how the course structure effectively supported both engagement and learning.

Table 7

Usability and Navigation

Theme	Defining Characteristics	Examples
Well-designed and User-friendly	Features a well-thought-out layout and user experience; easy to navigate	• "The training was good, and the quality of the site was very well designed." • "The information is laid out well and easy to navigate even for a novice like me." • "Some of the information is over my head, lol but overall content well laid out and easy to navigate."
Accessible and Understandable	Content is easy to access and understand	• "I found the entire user experience to be intuitive, interactive, pleasant, informative, and fascinating." • "The videos weren't overly intimidating because they weren't five hours long like some courses, I've taken over the years." • "The information is laid out very well. I was able to navigate through it easily." "I found the content easy to access and understand."

Summary

Chapter 4 presented an analysis of the survey data. Descriptive statistics underlined a strong belief in the importance of understanding cybersecurity and varying levels of confidence in identifying and protecting against cybersecurity threats. Qualitative feedback reinforced the positive reception of the course, with participants expressing increased cybersecurity awareness while suggesting areas for course improvement.

Chapter 5 discusses the implications of the case findings, offer recommendations for future research and course improvements, and further address the study's limitations.

CHAPTER 5

IMPLICATIONS AND CONCLUSIONS

Introduction

This chapter discusses the implications and conclusions drawn from the evaluation of the CS course. The primary goal of the case study was to understand participants' initial perceptions of cybersecurity practices and assess how the course improved their knowledge and preparedness. The findings, based on both quantitative and qualitative data, provide insights into the course's overall effectiveness and areas for potential improvement.

The chapter also demonstrates how the findings can inform future research and guide improvements in cybersecurity education. The limitations of the study are addressed by focusing on factors that may have influenced the results and their applicability. Finally, the practical and theoretical implications are explored and how the study potentially contributes to the field of cybersecurity education.

Research Discussion Overview

Data analysis revealed several key findings:

- Before the intervention, two-thirds of participants prioritized using strong passwords and enabling two-factor authentication.
- Participants reported limited confidence in identifying and protecting against threats before the intervention.
- Post intervention, participants reported having a better understanding of cybersecurity fundamentals and the threats that exist.
- Qualitative feedback consistently emphasized that the course was well-designed, user-friendly, and engaging.
- Some participants expressed a desire for more interactive, hands-on exercises.

Discussion

The Likert scale data provided important insights into participants' perceptions of the importance of cybersecurity. Before the intervention, participants overwhelmingly agreed that understanding cybersecurity is crucial, with an average score between “agree” and “strongly agree.” This result indicates a widespread recognition among participants of the significance of cybersecurity in their digital interactions. However, this recognition did not fully translate into confidence in applying this knowledge, as indicated by the lower pre-course survey confidence scores. Given the increasing frequency of cybersecurity threats in both personal and professional contexts, this strong belief in the importance of cybersecurity is still encouraging.

Additionally, before the intervention, participants reported only moderate engagement in proactively seeking out information about new cybersecurity threats and strategies, with their responses falling in the neutral zone. This indicates that while they may understand the importance of cybersecurity, they are not consistently taking active steps to stay informed about evolving threats. This mirrors concerns raised by IBM (2023), Sophos (2023), and Microsoft (2023), which emphasize that it is important that cybersecurity training be structured in a way that is comprehensible to all participants.

Despite this recognition of importance, participants expressed significantly lower confidence in their ability to identify and protect against cybersecurity threats. This challenge is compounded by the psychological tactics cybercriminals use, such as urgency, visual deception, and personalization (Longtchi et al, 2023). The average score for confidence was also in the neutral zone, suggesting that while participants are aware of the risks, many lack the practical skills necessary to address them effectively. This reflects the importance of hands-on education, as Habrusiev et al. (2023) point out, noting that structured learning environments are essential for

developing real-world skills. Similarly, Workman et al. (2022) emphasize that experiential learning is crucial for building confidence in identifying and responding to threats.

Post intervention, participants commented on the course's effective and engaging design which potentially contributes to the broad accessibility of the course. As one participant noted, the course was "very interesting and informative" with a "well-designed" layout that made the content accessible, even for those with limited technical knowledge. UDL (2020) emphasizes the importance of creating content that caters to a broad range of learner needs while making it accessible to those without technical expertise. This design philosophy follows the goals of the National Cybersecurity Agenda (2023) which calls for foundational cybersecurity skills across all sectors. Ensuring that cybersecurity education is both engaging and accessible is a critical step in building a workforce capable of handling cybersecurity threats as they emerge.

Concerning the course, participants responded positively, with one stating, "The curriculum was very effective, particularly in the way it re-reinforces the benefits of participating in various online communities," suggesting that the structure encouraged participants to seek out additional cybersecurity knowledge. Another participant appreciated the specific guidelines of the course, noting, "incorporating the information provided by NIST helps with understanding and implementing cybersecurity practices." Additionally, participants shared that, because of the course, they gained a "better understanding of what threats exist", and "how they could keep their devices up to date with the latest security patches." This post-course feedback demonstrates an increased understanding and intention to implement cybersecurity practices. As the majority of participants were from healthcare and business sectors, fields where cybersecurity training may not be a priority, these results reinforce the need for education that focuses on threat identification and response. These basic cybersecurity practices, as outlined by NIST (2020),

reduce user vulnerability to common cyber-attacks. This is particularly important in the context of the escalating costs of data breaches (IBM, 2023), where even small, proactive steps can dramatically reduce risk.

However, despite this positive reception, the lack of deeper, hands-on components may have limited participants' ability to fully engage with cybersecurity concepts beyond awareness. Constructive feedback pointed out areas for improvement, particularly the "lack of any hands-on exercise" and a desire for more interactive elements to help reinforce learning. One participant stated, "I find that I retain information better when I'm able to interact with the material," reflecting the importance of education that reinforces theoretical knowledge (Habrusiev et al., 2023; Workman et al., 2022). Ros et al. (2020) similarly advocate for the use of real-world simulations and interactive exercises and participants echoed this need in their feedback. Carley (2020) adds that social cybersecurity is also essential, as it examines how cyber-mediated factors, such as social engineering, shape user behavior. Integrating these aspects into training could enhance participants' ability to recognize and defend against these threats effectively. Given the complexity and increasing sophistication of cyberattacks, as described by Longtchi et al. (2023), incorporating exercises that simulate phishing attacks, malware, and credential theft would be beneficial in boosting participants' preparedness.

In summary, the case study survey findings reveal that while participants demonstrated a strong awareness of cybersecurity's importance, there were noticeable gaps in their confidence levels and proactive engagement. Although the participants recognized the importance of cybersecurity measures, many lacked the practical skills required for identifying threats and did not consistently seek out information on emerging risks. This suggests the need for training and ongoing education to maintain consistency between awareness and action in implementing

cybersecurity measures. Additionally, feedback from the eight participants who completed the course suggests that the program was effective in enhancing their cybersecurity knowledge. The course's structure, content delivery, and accessibility were well-received, aligning with the best practices advocated by frameworks like NICE (2020) and NIST (2020).

However, Lahcen et al. (2020) argue that awareness alone does not always result in action, particularly when human behaviors, such as biases or errors, are involved. Similarly, Sophos (2023) emphasizes the challenges organizations face in translating knowledge into consistent security practices, especially in sectors where cybersecurity resources may be limited. Participants emphasized the need for incorporating more hands-on, and interactive components to deepen their understanding of key concepts. This feedback aligns with current trends in cybersecurity education that stress practical application and continuous engagement (IBM, 2023; Microsoft, 2023). Incorporating these elements would further solidify the course's effectiveness in preparing participants to respond to real-world cybersecurity threats.

Limitations

Several limitations of this case study must be acknowledged. First, the sample size was relatively small, with only 15 participants completing the pre-course survey and eight participating in the post-course focus group discussion. This small sample size limits the generalizability of the findings. However, the study builds a foundation for future research and indicates the value of implementing the study with larger sample sizes to provide more robust and potentially generalizable results. Additionally, while efforts were made to capture a diverse demographic, the limited number of participants may not fully represent the range of backgrounds, education levels, and technology access within the broader Texarkana community.

This limitation may have influenced the findings, particularly regarding how different demographic factors affect perceptions and preparedness in cybersecurity.

Another limitation is the study's geographical context as it was conducted within the Texarkana area. The unique socio-economic and technological characteristics of this region may not reflect the conditions of other regions, further limiting the generalizability of the findings. Also, as the study relied on self-reported data from a single survey and focus group discussion questions, the possibility of response bias cannot be dismissed. Participants might have overstated their knowledge regarding cybersecurity or given answers that reflected what they thought was socially desirable.

The CS course, being an introductory course with a limited duration, may not have covered all aspects of cybersecurity practices comprehensively. Temporal factors, such as the timing of the course and the study, including any external events or developments in cybersecurity during this period, may have influenced participants' perceptions and attitudes. Addressing these limitations in future research could enhance the validity and reliability of the findings. In doing so, future studies could provide a clearer understanding of the effectiveness of cybersecurity training and offer a more accurate assessment of participants' preparedness.

Future Research

Future research should explore the long-term impact of cybersecurity education, such as the CS course, on participants' security behaviors. Longitudinal studies that track participants over extended periods would offer valuable insights into the lasting effects of these educational programs. By monitoring changes in cybersecurity practices over time, researchers could better understand whether participants maintain or improve their security habits post-training.

Expanding the sample size and including participants from diverse geographical regions and

industries would further enhance the generalizability of the findings and offer a broader perspective on the efficacy of cybersecurity education programs.

Additionally, investigating the effectiveness of different instructional approaches and teaching styles would be a valuable avenue for future research. Comparing outcomes from courses facilitated by various instructors could reveal key differences in teaching strategies and produce best practices for conveying complex cybersecurity concepts. Practical exercises, such as simulations of real-world cyberattacks, could be particularly effective in reinforcing theoretical knowledge. Another area to explore is the consistent application of essential cybersecurity practices. Despite participants' awareness of cybersecurity's importance, many still fail to implement these practices rigorously. Future research could investigate the underlying reasons for this gap and examine why well-informed users may not consistently follow critical cybersecurity measures. This line of inquiry is crucial, as it could lead to the development of targeted strategies that address these behavioral inconsistencies and enhance overall cybersecurity resilience.

Lastly, incorporating more rigorous statistical methods, such as moderation analysis or exploring interaction effects in regression models, could help identify factors that influence the effectiveness of cybersecurity education. This would allow researchers to assess how different variables, such as prior knowledge, occupation, or access to technology, interact to affect participants' learning outcomes.

Practical Implications

The practical implications of the course primarily relate to its effectiveness in increasing participants' cybersecurity knowledge and their preparedness in implementing key security practices. The course appeared to successfully promote the use of important cybersecurity

practices, such as MFA, which are critical for reducing security risks. If participants incorporate these practices into their routines, it could help strengthen security practices in personal and professional contexts, particularly in fields like healthcare and business, where safeguarding sensitive information is essential.

For organizations, the course provides an opportunity to better equip their workforce with fundamental cybersecurity knowledge. A more informed employee base may help reduce vulnerabilities caused by common security mistakes, thereby improving the organization's overall cybersecurity resilience. Additionally, the course provides a solid foundation for participants interested in advancing their education in cybersecurity. Incorporating the course into an organization's ongoing training efforts could reduce common security errors, such as weak password management or falling for phishing attacks, both of which are cited as frequent causes of breaches (IBM, 2023).

Lastly, the course's structure and content, which were well-received by participants, offer valuable insights into potential improvements for future training programs. While the course was informative, participants expressed a desire for more hands-on activities to deepen their understanding of cybersecurity concepts. They emphasized the need for real-life applications and exercises to better bridge the gap between theory and practice. Incorporating such experiential learning elements, like simulations or problem-solving activities, would not only make the material more engaging but also help participants internalize and apply cybersecurity concepts more effectively. This shift toward more experiential learning could also boost retention by helping participants maintain a higher level of preparedness long after the course is completed.

Theoretical Implications

The study contributes to the broader discourse on the intersection of human behavior and

cybersecurity. By showing the gap between participants' awareness of cybersecurity threats and their confidence in applying protective measures, this research adds to the growing body of literature that emphasizes the importance of behavioral and psychological factors in cybersecurity practices. As noted by Lahcen et al. (2020), human interaction with technology and the cognitive biases that influence decision-making are critical components in understanding vulnerabilities within cybersecurity systems. The study reinforces these ideas by demonstrating that, even with awareness of cybersecurity risks, participants may not fully engage with protective practices. This suggests that the theoretical models addressing cybersecurity must account for both knowledge acquisition and behavioral change.

The need for continuous and adaptive learning, as emphasized by connectivism (Siemens, 2005), is also underscored in this study. Connectivism suggests that learning is most effective when individuals can navigate and connect to various sources of information within a knowledge network. As cybersecurity threats are constantly evolving, participants' feedback regarding the need for more real-time, interactive elements supports the idea that learners must continually adapt to stay informed. This aligns with connectivism's emphasis on forming connections across diverse information sources to ensure up-to-date knowledge. The course's user-friendly design and focus on accessibility further reinforce the importance of staying current with the latest practices, adding to Siemens' emphasis on the importance of up-to-date learning in fields like cybersecurity. Additionally, this research supports the NIST Cybersecurity Framework (NIST (2020)), particularly in its focus on resilience through practical education. The NIST Framework's core functions of identify, protect, detect, respond, and recover, serve as a guide for building cybersecurity preparedness. The findings suggest that theoretical knowledge alone isn't enough; practical, hands-on training is necessary to ensure participants not only understand

cybersecurity concepts but also feel confident in applying them effectively.

Contributions to the Field

This study makes contributions to the field of learning technologies by exploring how connectivism (Siemens, 2005) and the NIST cybersecurity framework (NIST, 2020) can be integrated to enhance cybersecurity education. By focusing on these two frameworks, the research shows the importance of adaptive learning environments in preparing learners to navigate the shifting demands of cybersecurity. In highly technical fields like cybersecurity, connectivism's emphasis on building knowledge networks play an important role in engaging learners and promoting continuous learning.

The findings of this study reveal the critical role of hands-on, experiential learning in bridging the gap between theoretical knowledge and practical application of cybersecurity principles. While the course provided valuable insights, participants expressed a need for more real-life scenarios and exercises to solidify their understanding and skills. Aligning these practical elements with the NIST cybersecurity framework can ensure learners develop not just theoretical knowledge but also the confidence and competence required to implement cybersecurity practices in real-world environments. In doing so, the research offers a pathway for improving cybersecurity education so that learners are better able to apply their knowledge in applicable situations.

Conclusion

In conclusion, this case study examined the effectiveness of an introductory cybersecurity course designed for participants in the Texarkana region. By incorporating both quantitative data from a pre-course survey and qualitative feedback from a focus group discussion, the research explored participants' initial perceptions of cybersecurity practices and their knowledge and

preparedness after completing the course. While the study found that participants were generally aware of basic cybersecurity practices, they often lacked the confidence needed to apply them consistently. Focus group responses indicated the need for additional hands-on exercises to help enhance participants' skills and confidence. Although participants appreciated the course's clear structure and informative content, they indicated that additional interactive elements would help reinforce the theoretical knowledge gained.

Looking ahead, these findings suggest that future iterations of the course could benefit from incorporating more experiential learning components, such as simulations or real-world scenarios, to better meet participants' needs for practical application. While the study provides valuable observations, the relatively small sample size and focus on a specific geographic area should be considered when interpreting the results. Future research could expand on this work by exploring the long-term impact of cybersecurity education across a broader and more diverse population. Overall, the research emphasizes the need for instructional design to balance theoretical understanding with practical application in cybersecurity education. By addressing these gaps, future courses can more effectively prepare learners to apply their knowledge in real-world cybersecurity challenges.

APPENDIX A
IRB APPROVAL LETTERS

IRB #: IRB-24-129

Title: Cybersecurity in the Information Age: A Connectivist Approach to Instructional Design

Creation Date: 2-24-2024

End Date:

Status: **Approved**

Principal Investigator: Deborah Cockerham

Review Board: UNT IRB Full Board

Sponsor:

Study History

Submission Type	Initial	Review Type	Exempt	Decision	Exempt
-----------------	---------	-------------	--------	----------	---------------

Key Study Contacts

Member	Deborah Cockerham	Role	Principal Investigator	Contact	deborahcockerham@my.unt.edu
--------	-------------------	------	------------------------	---------	-----------------------------

Member	Michael Whisenant	Role	Primary Contact	Contact	lancewhisenant@my.unt.edu
--------	-------------------	------	-----------------	---------	---------------------------

Member	Michael Whisenant	Role	Investigator	Contact	lancewhisenant@my.unt.edu
--------	-------------------	------	--------------	---------	---------------------------

Application for Exempt Review

Name of Principal Investigator (PI): Michael Lance Whisenant Phone: 903-280-0825 (cell)

Status: ☐ faculty ☐ student ☒ staff ☐ other: _____ E-mail: Michael.whisenant@texarkanacollege.edu

Address where correspondence is to be sent: MWhisenant13@gmail.com

Title of Study: **Cybersecurity in the Information Age: A Connectivist Approach to Instructional Design**

If the PI is a student, provide the following student information:

Department: _____

Name & email address of faculty advisor: _____

Estimated beginning date of study: 4-15-24 Estimated duration of study: 1-2 weeks

Type of Project: ☒ thesis ☒ professional paper ☒ dissertation ☐ class project
(check all that apply) ☐ faculty research ☐ pilot ☐ other

Has project been submitted for funding (internal or external)? ☐ yes ☒ no

If yes, funding source: _____ (Proposal must be attached.)

Signatures:

Principal Investigator (PI): Signature certifies that the investigator has primary responsibility for all aspects of the research project.

Michael Whisenant

Principal Investigator

Date

Faculty Research Advisor (for student research only): Signature certifies that the faculty member has read, reviewed, and approved the content of the application and is responsible for the supervision of this research study. *

Faculty Research Advisor

Date

Academic Administrator: Signature certifies that the administrator has read, reviewed, and approved the content of the application. *

Dixon Boyles

Academic Administrator (Department Chair, Program Director, or Associate Dean)

March 22, 2024

Date

*waived if doctoral institution's SIGNED/APPROVED IRB application is included with this application

APPENDIX B
RECRUITMENT FLYER

UNIVERSITY OF NORTH TEXAS
The UNT
Department of Learning Technologies
Is conducting a Research Study on
Cybersecurity in the Information Age: A Connectivist Approach to Instructional Design
At Texarkana College

All participants will be 18 years or older.

You may qualify to participate in a research study that aims to bridge the identified gaps in literature and practice by developing an introductory cybersecurity curriculum that can be facilitated by interdisciplinary instructors in an online environment.

Eligible subjects will undergo a mixed-methods approach to investigate the impact of a cybersecurity education course on community members at Texarkana College (TC). By applying a quantitative survey alongside qualitative open-ended interviews, the research aims to assess participants' knowledge, attitudes, and cybersecurity practices, as well as any changes that occur as a result of engaging with the course content. The focus on community members provides a wide lens through which to examine the effectiveness of cybersecurity education.

Your participation in this research study involves an online pre-course survey that takes approximately five minutes and an in person post-course focus group that takes approximately 30 minutes for a total time of 35 minutes.

Subjects will not be compensated.

Principal Investigator: Deborah Cockerham
(940) 565-4470 (Office), deborah.cockerham@unt.edu

For more information, please contact Michael Lance Whisenant at Lancewhisenant@my.unt.edu

APPENDIX C

INFORMED CONSENT FOR STUDIES WITH ADULTS



UNIVERSITY OF NORTH TEXAS®

Informed Consent for Studies with Adults

TITLE OF RESEARCH STUDY: Cybersecurity in the Information Age: A Connectivist Approach to Instructional Design

RESEARCH TEAM: Michael Lance Whisenant, 903-280-0825, MWhisenant13@gmail.com

Principal investigator, Dr. Deborah Cockerham, (940) 565-4470 (Office),
deborah.cockerham@unt.edu

You are being asked to participate in a research study. Taking part in this study is voluntary. The investigators will explain the study to you and will answer any questions you might have. It is your choice whether or not you take part in this study. If you agree to participate and then choose to withdraw from the study, that is your right, and your decision will not be held against you.

You are being asked to take part in a research study about how educational sessions can empower community members with the necessary knowledge and skills to navigate the cyber threat landscape safely.

Your participation in this research study involves an online pre-course survey that takes approximately five minutes and an in person post-course interview that takes approximately 30 minutes for a total time of 35 minutes. More details will be provided in the next section.

You might want to participate in this study if you are interested in increasing your cybersecurity awareness. However, you might not want to participate in this study if you do not have time for the survey or interview.

You may choose to participate in this research study if you are 18 years of age or older and are enrolled in the Connected Security (CS) class at Texarkana College.

The reasonable foreseeable risks or discomforts to you if you choose to take part is confidentiality risks which you can compare to the possible benefit of providing valuable insights into the effectiveness of educational sessions in improving cybersecurity behaviors. This can inform future curriculum development and pedagogical strategies in the field. You will not receive compensation for participation.

DETAILED INFORMATION ABOUT THIS RESEARCH STUDY: The following is more detailed information about this study, in addition to the information listed above.

PURPOSE OF THE STUDY: The purpose of this paper is to design and evaluate an introductory cybersecurity course (referred to as Connected Security (CS) in this study) that is grounded in the Connectivism learning theory and the NIST Cybersecurity standards. This study aims to bridge the identified gaps in literature and practice by developing an introductory cybersecurity curriculum that can be facilitated by interdisciplinary instructors in an online environment.

TIME COMMITMENT: Participation in this study involves an online pre-course survey that takes approximately five minutes and an in person post-course focus group session that takes approximately 30 minutes for a total time of 35 minutes.

STUDY PROCEDURES: Participation in this study involves an online pre-course survey that takes approximately five minutes and an in person post-course focus group session that takes approximately 30 minutes for a total time of 35 minutes.

POSSIBLE BENEFITS: While there is no direct benefit to you, participants will potentially gain a deeper understanding of cybersecurity principles, thus learning how to protect their digital information effectively. Additionally, this may inform future curriculum development and pedagogical strategies in the field. You will not receive compensation for participation.

POSSIBLE RISKS/DISCOMFORTS: Participation in the online survey involves risks to confidentiality similar to a person's everyday use of the internet and that there is always a risk of breach of confidentiality. Otherwise, this research study is not expected to pose any additional risks beyond what you would normally experience in your regular everyday life.

This research study is not expected to pose any additional risks beyond what you would normally experience in your regular everyday life. However, if you do experience any discomfort, please inform the research team.

Participating in research may involve a loss of privacy and the potential for a breach in confidentiality. Study data will be physically and electronically secured by the research team. As with any use of electronic means to store data, there is a risk of breach of data security.

If you experience excessive discomfort when completing the research activity, you may choose to stop participating at any time without penalty. The researchers will try to prevent any problem that could happen, but the study may involve risks to the participant, which are currently unforeseeable. UNT does not provide medical services, or financial assistance for emotional distress or injuries that might happen from participating in this research. If you need to discuss your discomfort further, please contact a mental health provider, or you may contact the researcher who will refer you to appropriate services. If your need is urgent, helpful resources include If you need to discuss your discomfort further, please contact a mental health

provider, or you may contact the researcher who will refer you to appropriate services. If your need is urgent, helpful resources are:

Dr. Loudermill is our part-time Licensed Professional Counselor, and she provides counseling services in the areas of education, career, and personal issues. 903-823-3143/
tc.counselor@texarkanacollege.edu

Texarkana ER- 4646 Cowhorn Creek Rd, Texarkana, TX 75503
903-838-8000 / info@TexarkanaEmergencyCenter.com

COMPENSATION: There is no compensation for participating in this study.

CONFIDENTIALITY: Efforts will be made by the research team to keep your personal information private, including research study records, and disclosure will be limited to people who have a need to review this information. All paper and electronic data collected from this study will be stored in a secure location on the UNT campus and/or a secure UNT server for at least three (3) years past the end of this research. Research records will be labeled with a code and the master key linking names with codes will be maintained in a separate and secure location.

Participation in the online survey involves the potential for the loss of confidentiality similar to a person's everyday use of the internet.

The results of this study may be published and/or presented without naming you as a participant. The data collected about you for this study may be used for future research studies that are not described in this consent form. If that occurs, an IRB would first evaluate the use of any information that is identifiable to you, and confidentiality protection would be maintained.

While absolute confidentiality cannot be guaranteed, the research team will make every effort to protect the confidentiality of your records, as described here and to the extent permitted by law. In addition to the research team, the following entities may have access to your records, but only on a need-to-know basis: the U.S. Department of Health and Human Services, the FDA (federal regulating agencies), the reviewing IRB, and sponsors of the study.

This research uses a third-party software called SurveyMonkey and is subject to the privacy policies of this software noted here: <https://www.surveymonkey.com/mp/legal/privacy-policy/>

CONTACT INFORMATION FOR QUESTIONS ABOUT THE STUDY: If you have any questions about the study, you may contact Michael Lance Whisenant at 903-280-0825 or Dr. Deborah Cockerham at 940 565-4470 (Office). Any questions you have regarding your rights as a research subject, or complaints about the research may be directed to the Office of Research Integrity and Compliance at 940-565-4643, or by email at untirb@unt.edu.

CONSENT:

- ☐ I have read the consent information and agree to take part in the research.
- ☐ I have read the consent information and do not agree to take part in the research.

APPENDIX D
QUANTITATIVE SURVEY

Demographics

What is your age group? (CS1)

- 18-24 (1)
- 25-34 (2)
- 34-44 (3)
- 45-54 (4)
- 55-65 (5)
- 65+ (6)

What is your highest level of education completed? (CS2)

- High school or equivalent (1)
- Some college (2)
- Associate degree (3)
- Bachelor's degree (4)
- Master's degree (5)
- Doctoral degree (6)

Which field best describes your work or study area? (CS3)

- Information Technology (1)
- Education (2)
- Healthcare (3)
- Finance (4)
- Business (5)
- Other (please specify): (6)

Cybersecurity Construct (Self-Evaluation)

I believe that understanding cybersecurity is critical for my personal and professional life. (CS4)

- Strongly disagree (1)
- Disagree (2)
- Neither agree nor disagree (3)
- Agree (4)
- Strongly agree (5)

How confident are you in your ability to identify and protect cybersecurity threats? (CS5)

- Not at all confident (1)
- Not so confident (2)
- Somewhat confident (3)
- Very confident (4)
- Extremely confident (5)

I actively seek out information and resources to stay informed about the latest cybersecurity threats and protection strategies. (CS6)

- Strongly disagree (1)
- Disagree (2)
- Neither agree nor disagree (3)

- Agree (4)
- Strongly agree (5)

Best Practices Construct (Self-Evaluation)

Which of the following basic cybersecurity practices do you consider the most important in your digital life? (CS7)

- Using strong passwords (1)
- Enabling two-factor authentication (2)
- Regularly updating software (3)
- Using antivirus software (4)
- Avoiding public Wi-Fi for sensitive transactions (5)

Connectivism Construct (Self-Evaluation)

How familiar are you with the concept of Connectivism as a learning theory? (CS8)

- Not at all familiar (1)
- Not so familiar (2)
- Somewhat familiar (3)
- Very Familiar (4)
- Extremely familiar (5)

How often do you engage with online learning communities or networks to enhance your knowledge and skills? (CS9)

- Never (1)
- Rarely (2)
- Sometimes (3)
- Usually (4)
- Always (5)

APPENDIX E

FOCUS GROUP QUESTIONS

Overall Course Experience

- What were your overall impressions of the Connected Security course?
- How would you describe the design and layout of the course?

Content Understanding

- How has your understanding of cybersecurity threats and protective measures improved after taking this course?
- Can you share any specific parts of the course that helped you understand cybersecurity better?

Engagement and Usability

- Which parts of the course did you find most engaging or beneficial? Why?
- Were there any parts of the course that you found confusing or less engaging? How could these be improved?

Application of Knowledge

- How has the course influenced your ability to apply cybersecurity practices in your personal or professional life?
- Can you provide examples of how you have applied what you learned in the course to your daily digital behaviors?

Course Components

- How did you find the balance between theoretical knowledge and practical application in the course?
- Did you find the interactive elements, such as the CS-GPT, helpful in understanding the material?

Suggestions for Improvement

- Do you have any suggestions for improving the Connected Security course?
- How can the course better incorporate hands-on exercises or practical components?

REFERENCES

- Alsaleh, N. (2020). The effectiveness of an instructional design training program to enhance teachers' perceived skills in solving educational problems. *Educational Research Reviews*, 15(12), 751–763. <https://doi.org/10.5897/ERR2020.4082>
- Baeva, L. v. (2021). The “black swan” of covid-19 and the security issues in digital learning. *Galactica Media: Journal of Media Studies*, 2, 110–140.
- Barak, M., & Green, G. (2021). Applying a social constructivist approach to an online course on ethics of research. *Science and Engineering Ethics*, 27(1). <https://doi.org/10.1007/s11948-021-00280-2>
- Basie, V. S., & Rossouw, V. S. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, 26(1), 2-9. <https://doi.org/10.1108/ICS-04-2017-0025>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- Carley, K. M. (2020). Social cybersecurity: an emerging science. *Computational and Mathematical Organization Theory*, 26(4), 365–381. <https://doi.org/10.1007/s10588-020-09322-9>
- Center for Internet Security. (n.d.). *NIST Cybersecurity Framework Policy Template Guide*.
- Christensen, R., & Knezek, G. (2001). Instruments for assessing the impact of technology in education. *Computers in the Schools*, 18(2/3), 5–25.
- Christensen, R. (2002). Effects of technology integration education on the attitudes of teachers and students. *Journal of Research on Technology in Education*, 34(4), 411–433. <https://doi.org/10.1080/15391523.2002.10782359>
- Christensen, R., & Knezek, G. (2006). Pathway for preparing tomorrow's teachers to infuse technology. *Computers in the Schools*, 23(3–4), 1–21. https://doi.org/10.1300/J025v23n03_01
- Christensen, R., & Knezek, G. (2016). Validating the Technology Proficiency Self-Assessment Questionnaire for 21st Century Learning (TPSA C-21). *Journal of Digital Learning in Teacher Education*, 33(1), 20–31. <https://doi.org/10.1080/21532974.2016.1242391>
- CSRC Content Editor. (n.d.). *cybersecurity - Glossary* | CSRC. NIST Computer Security Resource Center. Retrieved October 29, 2023, from <https://csrc.nist.gov/glossary/term/cybersecurity>
- Coenraad, M., Pellicone, A., Ketelhut, D. J., Cukier, M., Plane, J., & Weintrop, D. (2020). Experiencing cybersecurity one game at a time: A systematic review of cybersecurity

- digital games. *Simulation and Gaming*, 51(5), 586–611.
<https://doi.org/10.1177/1046878120933312>
- Cohen, F. (1987). Computer viruses: Theory and experiments. *Computers & Security*, 6(1), 22–35. [https://doi.org/10.1016/0167-4048\(87\)90122-2](https://doi.org/10.1016/0167-4048(87)90122-2)
- Dewdney, A. K. (1984). Computer Recreations. *Scientific American*, 250(5), 14–23.
<https://doi.org/10.2307/24969361>
- Department of Defense (DoD). (1985). *Trusted computer system evaluation criteria*.
- Downes, S. (2008). Places to go: Connectivism & connective knowledge. *Innovate: Journal of Online Education*, 5(1). <https://nsuworks.nova.edu/innovate/vol5/iss1/6>
- du Toit-Brits, C. (2019). A focus on self-directed learning: The role that educators' expectations play in the enhancement of students' self-directedness. *South African Journal of Education*, 39(2). <https://doi.org/10.15700/saje.v39n2a1645>
- Fraenkel, J. R., Wallen, N. E., & Hyun, H. H. (2018). *How to design and evaluate research in education* (10th ed.). McGraw-Hill Education.
- Garber, L. (1999). Melissa virus creates a new type of threat. *Computer*, 32(6), 16–19.
- Garrison, D. R., Anderson, T., & Archer, W. (2010). The first decade of the community of inquiry framework: A retrospective. *Internet and Higher Education*, 13(1–2), 5–9.
<https://doi.org/10.1016/j.iheduc.2009.10.003>
- Goldie, J. G. S. (2016). Connectivism: A knowledge learning theory for the digital age? *Medical Teacher*, 38(10), 1064–1069. <https://doi.org/10.3109/0142159X.2016.1173661>
- Habrusiev, V. Yu., Tereshchuk, H. v., Stepanyuk, A. v., & Olendr, T. M. (2023). Pedagogical conditions for the formation of an effective information and learning environment in higher education institutions. *Information Technologies and Learning Tools*, 95(3), 183–196. <https://doi.org/10.33407/itlt.v95i3.5153>
- Heaton, J. (2004). *Reworking qualitative data*. SAGE Publications Ltd,
<https://doi.org/10.4135/9781849209878>
- IBM. (2023). *Cost of a data breach report 2023*.
- Joint Task Force. (2020). *Security and Privacy Controls for Information Systems and Organizations*. <https://doi.org/10.6028/NIST.SP.800-53r5>
- Karagiannis, S., & Magkos, E. (2020). Adapting CTF challenges into virtual cybersecurity learning environments. *Information and Computer Security*, 29(1), 105–132.
<https://doi.org/10.1108/ICS-04-2019-0050>

- Knight, P. (2000). ILOVEYOU: Viruses, paranoia, and the environment of risk. *The Sociological Review*, 48(2_suppl), 17–30. <https://doi.org/10.1111/j.1467-954x.2000.tb03518.x>
- Lahcen, M., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, 3(1). Springer Science and Business Media B.V. <https://doi.org/10.1186/s42400-020-00050-w>
- Latorre-Medina, M. J., & Tnibar-Harrus, C. (2023). Digital security in educational training programs: A study based on future teachers' perceptions. *Information Technologies and Learning Tools*, 95(3), 102–111. <https://doi.org/10.33407/itlt.v95i3.5204>
- LaTour, K. A., & Noel, H. N. (2021). Self-directed learning online: An opportunity to binge. *Journal of Marketing Education*, 43(2), 174–188. <https://doi.org/10.1177/0273475320987295>
- Li, N., Zhang, Z., Che, X., Guo, Z., & Cai, J. (2021). A survey on feature extraction methods of heuristic malware detection. *Journal of Physics: Conference Series*, 1757(1). <https://doi.org/10.1088/1742-6596/1757/1/012071>
- Lukasik, S. J. (2011). Why the ARPANET was built. *IEEE Annals of the History of Computing*, 33(3), 4–20. <https://doi.org/10.1109/MAHC.2010.11>
- Mailloux, L. O., & Grimaila, M. R. (2018). Advancing cybersecurity. *IEEE Computer Society*, 51(6), 1–8. <https://doi.org/10.1109/MC.2018.3191240>
- Mcgriff, S. J. (2000). *Instructional System Design (ISD): Using the ADDIE Model Analysis*. http://www.seas.gwu.edu/~sbraxton/ISD/general_phases.html
- Microsoft. (2022). *Microsoft digital defense report 2022*.
- Microsoft. (2023). *Microsoft digital defense report building and improving cyber resilience*.
- Microsoft Copilot. (2023). *Generated Responses*. Microsoft. <https://www.microsoft.com/en-us/>
- Morales, C., Knezek, G., & Christensen, R. (2008). Self-efficacy ratings of technology proficiency among teachers in Mexico and Texas. *Computers in the Schools*, 25(1–2), 126–144. <https://doi.org/10.1080/07380560802158004>
- National Academies of Sciences, E. (2019). *A decadal survey of the social and behavioral sciences: A research agenda for advancing intelligence analysis*.
- National Initiative for Cybersecurity Education. (2020). *NICE strategic plan*. www.nist.gov/nice
- National Institute of Standards and Technology. (2017, June). *NIST Special Publication 800-63B*. Retrieved October 3, 2023, from <https://pages.nist.gov/800-63-3/sp800-63b.html>
- National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. <https://doi.org/10.6028/NIST.CSWP.04162018>

- NIST. (2023, March 16). *The Five Functions* | NIST. Cybersecurity Framework. Retrieved October 3, 2023, from <https://www.nist.gov/cyberframework/online-learning/five-functions#identify>
- Neumann, K. L., Alvarado-Albertorio, F., & Ramírez-Salgado, A. (2021). Aligning with Practice: Examining the Effects of a Practice-Based Educational Technology Course on Preservice Teachers' Potential to Teach with Technology. *TechTrends*, 65(6), 1027–1041. <https://doi.org/10.1007/s11528-021-00672-y>
- Nolan-Grant, C. R. (2019). The community of inquiry framework as learning design model: A case study in postgraduate online education. *Research in Learning Technology*, 27. <https://doi.org/10.25304/rlt.v27.2240>
- Office of the National Cyber Director. (2023, July 31). FACT SHEET: Biden-Harris administration announces National Cyber Workforce and Education Strategy, unleashing America's cyber talent. *The White House*. Retrieved November 8, 2023, from <https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/31/fact-sheet-biden-harris-administration-announces-national-cyber-workforce-and-education-strategy-unleashing-americas-cyber-talent/>
- Owen, J., & Wasiuk, C. (2021). An agile approach to co-creation of the curriculum. *International Journal for Students as Partners*, 5(2), 89–97. <https://doi.org/10.15173/ij sap.v5i2.4475>
- Pan, X. (2020). Technology acceptance, technological self-efficacy, and attitude toward technology-based self-directed learning: Learning motivation as a mediator. *Frontiers in Psychology*, 11. <https://doi.org/10.3389/fpsyg.2020.564294>
- Payne, B. K., He, W., Wang, C., Wittkower, D. E., & Wu, H. (2021). Cybersecurity, technology, and society: Developing an interdisciplinary, open, general education cybersecurity course. *Journal of Information Systems Education*, 32(2), 134-149.
- Robson, C., & McCartan, K. (2016). *Real world research* (4th ed.). Wiley.
- Ros, S., Gonzalez, S., Robles, A., Tobarra, L. L., Caminero, A., & Cano, J. (2020). Analyzing students' self-perception of success and learning effectiveness using gamification in an online cybersecurity course. *IEEE Access*, 8, 97718–97728. <https://doi.org/10.1109/ACCESS.2020.2996361>
- Russell, A. L. (1995). Stages in learning new technology: Naive adult email users. *Computers & Education*, 25(4), 173–178. [https://doi.org/10.1016/0360-1315\(95\)00073-9](https://doi.org/10.1016/0360-1315(95)00073-9)
- Sanger, C. S. (2020). Inclusive pedagogy and universal design approaches for diverse learning environments. In *Diversity and inclusion in global higher education: Lessons from across Asia* (pp. 31–71). Springer Singapore. https://doi.org/10.1007/978-981-15-1628-3_2

- Sahay, M. (2023, October 28). Who invented the antivirus? A history of antivirus software. *PCInsider*. Retrieved November 4, 2023, from <https://www.thepecinsider.com/who-invented-antivirus-history-timeline-evolution/>
- Samociuk, D. (2023). Antivirus evasion methods in modern operating systems. *Applied Sciences (Switzerland)*, 13(8). <https://doi.org/10.3390/app13085083>
- Sharma, A., & Nazir, S. (2021). Assessing the technology self-efficacy of maritime instructors: An explorative study. *Education Sciences*, 11(7), 1–14. <https://doi.org/10.3390/educsci11070342>
- Siemens, George. (2005). Connectivism: A learning theory for the digital age. *Instructional Technology & Distance Learning*, 2(1), 1–9.
- Spatioti, A. G., Kazanidis, I., & Pange, J. (2022). A comparative study of the ADDIE instructional design model in distance education. *Information*, 13(402), 1–20. <https://doi.org/10.3390/info13090402>
- Sophos. (2023). *The State of ransomware 2023*.
- Stephen Downes. (2006, August 29). *An introduction to connective knowledge*. <https://www.Downes.ca/Cgi-Bin/Page.Cgi?Post=33034>.
- Texas Higher Education Coordinating Board. (2022). Information technology security. *Workforce Education Course Manual*. Retrieved October 2, 2023, from <http://thecb.state.tx.us/apps/workforceed/wecm/>
- United States Census Bureau. (2022). QuickFacts: Texarkana city, Texas; Texarkana city, Arkansas. *U.S. Department of Commerce*. Retrieved February 25, 2024, from <https://www.census.gov/quickfacts/fact/table/texarkanacityarkansas,texarkanacitytexas/PST045222#PST045222>
- U.S. Bureau of Labor Statistics. (2023, September 6). Information security analysts: Occupational outlook handbook. Retrieved September 27, 2023, from <https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-1>
- Whisenant, L., & Bradshaw-Ward, D. (2021). Technological proficiency: Do non-traditional students have the technological skills to be successful in college? *13th International Conference on Education and New Learning Technologies*, 10517–10523.
- Whisenant, L. (2022). Information security and digital rights management: A brief literature review. *ICERI 2022 Conference*, 76–80.
- Whisenant, L. (2022). Technology and the instructor: Where to now? *ICERI 2022 Conference*, 66–75.

Workman, M. D., Anthony Luevanos, J., & Mai, B. (2022). A study of cybersecurity education using a present-test-practice-assess model. *IEEE Transactions on Education*, 65(1), 40–45. <https://doi.org/10.1109/TE.2021.3086025>

Woszczynski, A. B., Pridmore, J. L., Bandyopadhyay, T., Godin, J., & Prince, B. J. (2021). Agile course design: Multi-university faculty collaboration to design the IS course for an online MBA program. *Journal of Information Systems Education*, 32(1), 9–26. <http://agilemanifesto.org/>