CYBEREDUCATION-BY-DESIGN™: DEVELOPING A FRAMEWORK FOR CYBERSECURITY EDUCATION AT SECONDARY EDUCATION INSTITUTIONS IN ARIZONA

Paul Wagner

Follow this and additional works at: https://scholar.dsu.edu/theses
CYBEREDUCATION-BY-DESIGN™: DEVELOPING A FRAMEWORK FOR CYBERSECURITY EDUCATION AT SECONDARY EDUCATION INSTITUTIONS IN ARIZONA

A dissertation submitted to Dakota State University for the degree of

Doctor of Philosophy

in

Cyber Defense

May 19, 2023

By
Paul Wagner

Dissertation Committee:

Dr. Kevin Streff
Dr. Bhaskar Rimal
Dr. Mark Hawkes
DISSERTATION APPROVAL FORM

This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Philosophy degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

Student Name: Paul Wagner

Dissertation Title: CYBEREDUCATION-BY-DESIGN™: DEVELOPING A FRAMEWORK FOR CYBERSECURITY EDUCATION AT SECONDARY EDUCATION INSTITUTIONS IN ARIZONA

Dissertation Chair/Co-Chair: Kevin Streff
Name: Kevin Streff
Date: May 23, 2023

Dissertation Chair/Co-Chair: 
Name: 

Committee member: Bhaskar Rimal
Name: Bhaskar Rimal
Date: May 23, 2023

Committee member: Mark Hawkes
Name: Mark Hawkes
Date: May 23, 2023

Committee member: 
Name: 

Committee member: 
Name: 

Original to Office of Graduate Studies and Research
Acid-free copies with written reports to library.
ACKNOWLEDGEMENT

My cybersecurity academic journey began in the Fall of 2017 when I enrolled in my MS in Cybersecurity. Since that time, countless hours were spent on coursework, certifications, reading, research, and writing, culminating in this dissertation and my Ph.D. These hours meant less time with family, and I want to wholeheartedly thank my wife, Karen, son, Ethan, and daughter, Allison, for their love and support over these years. I also want to thank my parents, Thomas and Barbara, for their enduring support along the many journeys I have taken. I want to particularly thank my father for his example of endurance and hard work in the face of adversity. You have been a true inspiration.

I also want to highlight the support of Ms. Janet Hartkopf, program director for the cybersecurity programs at Basha and Chandler High Schools. I would not have been able to collect the data and complete this dissertation without your support. Your dedication to your students and cybersecurity education in the K-12 space is an example for Arizona and the nation. You are a true champion for cybersecurity education.

To my dissertation committee, including my Chair, Dr. Kevin Streff, and members, Dr. Mark Hawkes, and Dr. Bhaskar Rimal – thank you for your support, insights, and time throughout the program and the dissertation process. It has been an honor learning and working with you. Finally, I want to thank my family, friends, mentors, and colleagues. There are too many to name; however, each of you has pushed me to achieve excellence during my military and academic careers.
ABSTRACT

Most survey results agree that there is a current and ongoing shortage of skilled cybersecurity workers that places our privacy, infrastructure, and nation at risk. Estimates for the global Cybersecurity Workforce Gap range from 2.72 million (ISC2, 2021) to 3.5 million (Cyber Academy, 2021) for 2021 and the United States estimates range from 465,000 (Brooks, 2021) to over 769,000 (Cyber Seek, 2022) open jobs as of November 2022. The most optimistic estimates still demonstrate a critical issue. As cybersecurity threats continue to grow in sophistication, scope, and scale, the ability to secure the United States from these threats lies in the ability to develop cybersecurity professionals with the knowledge, skills, and abilities (KSAs) to accomplish the tasks associated with their cyber roles. The ability to supply qualified cybersecurity professionals is outpaced by the growing demand as previously outlined. This study proposes that conducting a case study of existing cybersecurity programs at secondary education institutions can identify the critical elements of these programs. These elements can be codified into program profiles and further refined into a comprehensive cybersecurity education framework for secondary education institutions. This framework can be used by school districts throughout Arizona to develop cybersecurity programs and ultimately develop qualified and competent cybersecurity professionals to overcome the cybersecurity workforce gap.
DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions, or writings of another.

I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

[Signature]

Paul Wagner
# TABLE OF CONTENTS

**DISSENTATION APPROVAL FORM**  
**ACKNOWLEDGEMENT**  
**ABSTRACT**  
**DECLARATION**  
**TABLE OF CONTENTS**  
**LIST OF TABLES**  
**LIST OF FIGURES**  

## CHAPTER 1 Introduction  
1.1 Background of the Problem  
1.2 Statement of the Problem  
1.3 Purpose of the Project  
1.4 Rationale  
1.5 Research Questions  
1.6 Significance of the Project  

## CHAPTER 2 Literature Review  
2.1 Government Legislation  
2.2 Standards Organizations  
2.3 Curriculum  
2.4 Current Solutions  
2.5 Literature Review Synopsis  

## CHAPTER 3 Research Methodology  
3.1 Research Approach  
3.2 Context  
3.3 Research Design  

## CHAPTER 4 Analysis, Results, and Discussion  
4.1 Program Profiles  
4.2 Initial Interview Results and Analysis  
4.3 CyberEducation-by-Design Framework  
4.4 Framework Interview Results and Analysis
LIST OF TABLES

Table 1: Organization Crosswalk.................................................................................................................. 30
Table 2: Draft Program Profile ...................................................................................................................... 40
Table 3: Chandler AZ Demographics (Census, 2022) .................................................................................. 45
Table 4: Chandler Unified District Demographics (US News, 2019) ............................................................... 45
Table 5: Basha High School General Demographics (Basha, 2021) ............................................................... 46
Table 6: Formal Learning Activity Materials and Fees .................................................................................... 50
Table 7: Chandler High School General Demographics (Chandler, 2021) ....................................................... 54
Table 8: Interview Recommendations, Opportunities, and Challenges ....................................................... 65
Table 9: Non-Formal and Informal Learning Activity Examples ................................................................. 69
LIST OF FIGURES

Figure 1: Building Blocks for a Capable and Ready Workforce (Newhouse, 2017) .................. 15
Figure 2: NCAE-C Program of Study (PoS) Evaluation Conceptual Model (NCAEC, 2021) .... 16
Figure 3: CSEC Thought Model (CSEC, 2017) ................................................................. 18
Figure 4: Big Idea #1 Ethics: High School Cybersecurity Curriculum Guidelines (Dark, 2021) 19
Figure 5: K-12 Cybersecurity Learning Standards Core Themes (Cyber.org, 2021) ............... 21
Figure 6: Multi-Level, Multi-Discipline Cyber Education Approach (Sobiesk, 2015) .......... 24
Figure 7: Factors Impacting the Maintenance of Cybersecurity Certifications (Knapp, 2017) ..26
Figure 8: Internship and Apprenticeship Differences (Stoker, 2021) .................................. 27
Figure 9: Basha Cyber Program Student Enrollment ......................................................... 47
Figure 10: Basha High School Cybersecurity Program Graduates ...................................... 47
Figure 11: Basha High School and Cybersecurity Program Demographics ....................... 48
Figure 12: Chandler Cyber Program Student Enrollment .................................................... 55
Figure 13: Chandler High School Cybersecurity Program Graduates .................................. 55
Figure 14: Chandler High School and Cybersecurity Program Demographics .................... 56
Figure 15: Separate Learning Paths .................................................................................. 66
Figure 16: Combined Learning Paths ................................................................................ 67
Figure 17: U. S. Education Levels (USA Hello, 2023) ....................................................... 68
Figure 18: Formal Learning Delineation ............................................................................. 68
Figure 19: Non-Formal and Informal Learning Integration ................................................. 69
Figure 20: Non-Formal and Informal Learning Activity Examples ..................................... 72
Figure 21: Computing Systems Concepts, Standards, and Learning Objectives Crosswalk ....75
Figure 22: Digital Citizenship Concepts, Standards, and Learning Objectives Crosswalk ....76
Figure 23: Security Concepts, Standards, and Learning Objectives Crosswalk ................. 76
Figure 24: Post-Secondary Pathway Options .................................................................... 79
Figure 25: Comprehensive CyberEducation-by-Design Framework .................................... 81
CHAPTER 1

Introduction

1.1 Background of the Problem

Cybersecurity is critical to individuals and organizations globally. The United States (U.S.) faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people’s security and privacy (Biden, 2021). This is evidenced by the Colonial Pipeline Attack (Turton, 2021); SolarWinds Attack (CIS, 2021); and ransomware attacks against healthcare systems (Weiner, 2021), U.S. schools and colleges (Kshertri, 2021), and critical infrastructure (Cluley, 2021).

Most survey results agree that there is a current and ongoing shortage of skilled cybersecurity workers that places our privacy, infrastructure, and nation at risk. Estimates for the global Cybersecurity Workforce Gap range from 2.72 million (ISC2, 2021) to 3.5 million (Cyber Academy, 2021) for 2021 and the United States estimates range from 465,000 (Brooks, 2021) to over 769,000 (Cyber Seek, 2022) open jobs as of November 2022. The most optimistic estimates still demonstrate a critical issue.

Additionally, cybersecurity threats continue to grow in sophistication, scope, and scale. The ability to secure the U.S. from these threats lies in the ability to develop cybersecurity professionals with the knowledge, skills, and abilities (KSAs) to accomplish the tasks associated with their cybersecurity roles. The ability to supply qualified cybersecurity professionals is outpaced by the growing demand as previously outlined. Solving the demand problem relies on several stakeholders including K-12 education institutions, post-secondary education institutions,
employers, and the aspiring cybersecurity professional. There are opportunities and limitations identified with each of these stakeholders’ ability to address the underlying issue.

1.1.a K-12 Education

At a fundamental level, cybersecurity education is, “providing students with an understanding of how connected electronic devices interact in a digital age, how to protect digital assets from vulnerabilities and the moral and ethical issues surrounding the uses of technology in our society.” (Cyber.org, 2020). K-12 education institutions have a key role in addressing the cybersecurity professional shortage in two primary ways. First, K-12 education provides the ability to raise awareness and interest in cybersecurity. Second, it provides a conduit for fundamental knowledge needed to pursue post-secondary education or career pathways in this field. However, nationally there is a lack of quality Science, Technology, Engineering, and Math (STEM) programs, which cybersecurity is part of; lack of accessibility by all students, specifically minority students and students from lower Socio-Economic Status (SES); and overall stagnant performance in STEM assessments (Burke, 2021). Additionally, 75% of recent high school graduates feel they are underprepared to make college and career decisions (Lucariello, 2022) and are underprepared to enter the workforce (Lim, 2019). Further, the results of a 2020 national survey on the state of cybersecurity education in K-12 schools identified the following:

- Most K-12 educators do not know a lot about cybersecurity education.
- Cybersecurity deserts associated with inequitable access to cybersecurity education persist.
- Most students know little or nothing about cybersecurity.
- Access to cybersecurity education is infrequent and uneven.
• Cybersecurity education is rarely a focus of extracurriculars despite student interest.
• Cyberbullying and Terrorism are the most frequent cybersecurity education topics in K-12 schools (Cyber.org, 2020).

1.1.b Post-Secondary Education

The lack of cybersecurity awareness and education continues in post-secondary education. The output from secondary education is lacking the ability to solve the cybersecurity workforce problem. Graduation statistics from 2020 identified approximately one million graduates earning an associate’s degree, approximately two million graduates earning a bachelor’s degree, and approximately one million graduates earning an advanced degree (master’s, doctorate, or professional degree) (Hanson, 2022). Despite the increasing availability of cybersecurity programs in secondary education institutions, the overall percentage of college graduates having cybersecurity-related skills is low. The most recent data provided by the National Center for Education Statistics determined that only three percent of college graduates earned a degree in computer and information sciences (Kroll, 2019). Additionally, a Center for Strategic and International Study survey identified only 23 percent of IT employers felt that cybersecurity-related education programs were preparing students for cybersecurity roles (Crumpler, 2019). Similarly, an ISACA survey found that 61 percent of organizations believe that fewer than half of all cybersecurity applicants are qualified for the job (Crumpler, 2019). Finally, 80 percent of hiring managers do not believe that four-year degrees prepare graduates for cybersecurity roles due to the lack of hands-on training integrated into cybersecurity degrees (Crumpler, 2019). This leads to capacity and competency issues for students completing degrees at post-secondary education institutions.
1.1.c Employers

Employers have a dual role in the cybersecurity workforce problem. They are the demand aspect for the output of training and educational institutions. This demand is not only for cybersecurity professionals, but those cybersecurity professionals graduating with cybersecurity degrees who can design secure systems, create new tools for defense, and hunt down hidden vulnerabilities in software and networks (Crumpler, 2019). As hiring managers, these employers maintain some of the responsibility for changing their hiring practices. Employers need to be realistic with their job postings, create entry-level positions as required that align with those KSAs at the appropriate level, and work with education institutions to provide internship and apprenticeship programs. Finally, the cost of training a cybersecurity workforce can be a barrier for many organizations potentially leaving them vulnerable without adequate workforce or talent.

1.1.d Aspiring Cybersecurity Professional

Without the mechanisms from educational institutions or through the workplace, aspiring cybersecurity professionals can develop their KSAs through non-formal and informal learning activities. These learning activities within the cybersecurity content area are abundantly available. Individuals can self-study to develop their KSAs or leverage content providers to guide them. Opportunities consist of publicly available study material, “gamified” learning platforms like TryHackMe and HackTheBox, certification bodies that provide training aligned with their industry certifications, boot camps, student camps, and other learning activities. Despite their value, there are some issues with these limited or non-structured learning activities. For example, with gamified learning platforms, the lack of industry-recognized certification or academic credentials can be a limiting factor in employability. Industry certifications are continually debated on their value, necessity, and ability to accurately quantify an individual’s
KSAs. Industry certifications are broadly categorized as vendor-neutral and vendor-specific. Vendor-neutral certifications: such as those offered by CompTIA, (ISC)2, and ISACA; demonstrate broad competencies of cybersecurity concepts, technologies, tools, and processes. Vendor-specific certifications: such as those provided by Cisco, Microsoft, and Amazon; validate the knowledge and skills associated with specific security platforms, tools, and techniques requiring the demonstration of expertise on a specific tool or platform. There are hundreds of certification options as depicted by the image from Paul Jerimy’s site which is found in Appendix B. Another avenue for self-development is cybersecurity boot camps. The growth of cybersecurity boot camps has introduced fraud, false promises, and poor quality from some of these vendors. Many boot camps allude to or even promise employment upon completion of their program. For example, CCS Learning Academy’s website states, “No course on earth can give you 100% job guarantee, but going through a cybersecurity boot camp boosts your employability by nearly 99%. Boot camp grads can expect an entry-level position in cybersecurity after completing the course.” (CCS Learning Academy, 2021).

These approaches to cybersecurity education and training take different and typically siloed approaches with minor or unintentional overlap. The resolution of the cybersecurity workforce gap continues to widen despite the myriad of different opportunities for developing cybersecurity professionals. The current solutions do not resolve the capacity problem, nor does it provide the talent desired by employers. Additionally, each of these stakeholders has a role in solving the cybersecurity workforce shortage or developing the skills of current cybersecurity professionals in the field. Thus, a better approach to resolving this problem is required. Synergy can be obtained by integrating opportunities, approaches to learning, and collaboration among
stakeholders. The solution should be comprehensive. The term “comprehensive” for this study will include the following attributes: modular, scalable, rigorous, and accessible.

1.2 Statement of the Problem

Comprehensive cybersecurity education programs are significantly lacking in secondary education environments to meet the growing demand for cybersecurity professionals.

1.3 Purpose of the Project

The purpose of this project is to create comprehensive program profiles of existing cybersecurity education programs at secondary education institutions in Arizona. These program profiles will inform the development of a proposed comprehensive cybersecurity education framework for secondary education institutions that can be adopted by school districts throughout Arizona. The framework will incorporate formal, non-formal, and informal learning activities aligned to defined standards, curricular guidelines, and learning objectives.

Project Objectives

1. Develop cybersecurity education program profiles of existing cybersecurity programs in Arizona.


3. Evaluate the CyberEducation-by-Design Framework against the developed program profiles and survey results.

1.4 Rationale

Educational laws, policies, standards, guidelines, and implementation vary greatly among states and can vary at different levels across districts within the same state. This creates a
challenge when implementing programs, especially programs that are outside traditional subject areas of English, Mathematics, Science, and Social Studies. Until recently, the supporting guidance and funding for cybersecurity education has been focused on post-secondary education institutions. For example, Cyber.org published version 1.0 of the K-12 Cybersecurity Learning Standards in August of 2021 (Cyber.org, 2021). Similarly, Teach Cyber published the High School Cybersecurity Curriculum Guidelines & Glossary in 2021 (Dark, 2021). The shift in focus to the K-12 space for cybersecurity education and the publication of these seminal documents provides an opportunity to leverage secondary education institutions to address the cybersecurity professional workforce gap.

1.5 Research Questions

1. What are the elements of program profiles of existing cybersecurity education programs at secondary education institutions in Arizona?

2. What are the elements of a CyberEducation-by-Design framework that supports cybersecurity education at secondary education institutions in Arizona?

3. Do the program profiles and provide the ability to develop the CyberEducation-by-Design Framework?

1.6 Significance of the Project

This study is important because there is limited information on how cybersecurity education programs at secondary education institutions and what elements these programs are comprised of. Additionally, a comprehensive framework for cybersecurity education doesn’t exist at any level and existing support for secondary education institutions is limited and sporadically implemented. Although the study will focus on secondary education institutions in
Arizona, the intent is that the program profiles and proposed framework can be applied nationally. The study will conduct a case study analysis of cybersecurity programs in Arizona to develop program profiles. These program profiles will identify program elements and requirements for implementing a cybersecurity education program at secondary education institutions; how formal, non-formal, and informal learning activities can be integrated to produce capacity and competency in prospective cybersecurity professionals; and codify disparate elements into a framework for use by secondary education institutions.

Additionally, the program profiles developed based on the cybersecurity programs at secondary education institutions in Arizona can be used to develop program profiles for cybersecurity education programs at secondary education institutions nationally. These program profiles can be used as a library of artifacts to expand cybersecurity programs nationally.
CHAPTER 2

Literature Review

A Systematic Literature Review (SLR) technique was used to find relevant articles from 2010 to 2023. Relevant information was extracted from select articles to inform analysis and discussion. A variety of sources were used to identify relevant sources for this research including Google Scholar, IEEE, Elsevier, EBSCO, Proquest, and other library resources. Search terms included but were not limited to the term “cybersecurity” and combining “cybersecurity” with standards, guidelines, education, K-12 education, legislation, dual enrollment, certifications, and safety.

Given the limited, specific research on K-12 cybersecurity education and its application to current cybersecurity workforce shortages, a liberal inclusive set of search criteria was used. Full-text journal articles were used to identify and analyze current initiatives in cybersecurity education and training within the K-12 space and current issues with cybersecurity workforce development. Information from these articles was extrapolated for their potential use in developing the program profiles and CyberEducation-by-Design framework. Editorials, trade journals, and other online resources were used to identify the latest statistics, applications, and concerns facing cybersecurity education and workforce development.

2.1 Government Legislation

Arguably, “Cybercrime” and the need for cybersecurity professionals have been around for nearly two centuries. One of the first examples occurred in 1834 when a pair of thieves hacked the French Telegraph System to steal financial market information (Herjavec, 2019).
Cybercrime and cyber warfare have become more commonplace and sophisticated since then. Despite this long need for cybersecurity professionals, it wasn’t until President Reagan signed into law the Computer Security Act of 1987 directing the National Bureau of Standards to, “establish a computer standards program for Federal computer systems, including guidelines for the security of such systems drawing on technical security guidelines developed by the National Security Agency (NSA).” (Glickman, 1988, p. 6). President Clinton established the President’s Commission on Critical Infrastructure Protection in 1996 and released the first national strategy for protecting the nation’s computer networks from attack in 2000 (Clinton, 2000).

In 2003, President Bush released The National Security Strategy to Secure Cyberspace which articulated five national priorities:

1. A National Cyberspace Security Response System,
2. A National Cyberspace Security Threat and Vulnerability Reduction Program,
3. A National Cyberspace Security Awareness and Training Program,
4. Securing Governments’ Cyberspace, and

Four major actions and initiatives tied to “Priority 3” which directly relates to this research include:

1. Promote a comprehensive national awareness program to empower all Americans; businesses, the general workforce, and the general population, to secure their parts of cyberspace,
2. Foster adequate training and education programs to support the nation’s cybersecurity needs,
3. Increase the efficiency of existing general cybersecurity training programs, and
4. Promote private-sector support for well-coordinated, widely recognized professional cybersecurity certifications (Bush, 2003).

President Obama led many initiatives to improve the nation’s cybersecurity. These initiatives include the Cyberspace Policy Review (2009), making U.S. Cyber Command permanent (2009) (Armerding, 2013), issuing Executive Order 13636, “Improving Critical Infrastructure Cybersecurity (2013),” which led to the National Institute of Standards and Technology (NIST) development of the Cybersecurity Framework (2014) (Obama, 2013), and the development of the Cybersecurity Act which includes Cybersecurity Information Sharing, National Cybersecurity Advancement, Federal Cybersecurity Workforce Assessment, and a variety of other cyber matters (2015) (Obama, 2015). Additionally, President Obama implemented the Cybersecurity National Action Plan (CNAP) which established the Commission on Enhancing Cybersecurity, modernize government IT, and empower Americans to secure their online accounts (CNAP, 2017). CNAP enhanced cybersecurity education and training, through the National Initiatives for Cybersecurity Education (NICE) to expand Scholarship for Service opportunities, develop a cybersecurity core curriculum, and strengthen the National Centers for Academic Excellence in Cybersecurity (NCAE-C) Program.

President Trump issued Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, which focused on modernizing federal information technology infrastructure, working with state and local government and private sector partners to more fully secure critical infrastructure, and collaborating with foreign allies (CISA, 2020). In response to this, the Department of Commerce and Department of Homeland Security investigated cybersecurity workforce development determining the following:

- The U.S. cybersecurity workforce needs immediate and sustained improvements,
• It is necessary to expand the pool of cybersecurity candidates through retraining and by increasing the participation of women, minorities, and veterans,
• There is a shortage of cybersecurity teachers at the primary and secondary levels, faculty in higher education, and training instructors, and
• Comprehensive and reliable data about cybersecurity workforce position needs and education and training programs are lacking (CISA, 2020).

Most recently, President Biden issued his Executive Order to improve U.S. cybersecurity which focuses on removing barriers to threat information sharing between government and the private sector, improving software supply chain security, establishing a cybersecurity safety review board, creating a standard playbook for responding to cybersecurity incidents, improve detection of cybersecurity incidents on federal government networks, and improve investigative and remediation capabilities (Biden, 2021). Additionally, the K-12 Cybersecurity Act of 2021 was signed into law ordering the Cybersecurity and Infrastructure Security Agency (CISA) to analyze how cybersecurity risks specifically impact K-12 educational institutions, conduct an evaluation of the challenges K-12 educational institutions face in securing information systems and student records and implementing cybersecurity protocols, identifying cybersecurity challenges relating to remote learning, and evaluate the most accessible ways to communicate cybersecurity recommendations and tools (Peters, 2021).

2.2 Standards Organizations

Several standards organizations are involved in overcoming the cybersecurity workforce gap in response to or in support of these government initiatives. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-181, Workforce Framework for Cybersecurity (National Initiatives for Cybersecurity Education (NICE) Framework), provides a
set of building blocks for describing the tasks, knowledge, and skills (TKS) that are needed to perform cybersecurity work performed by individuals and teams for employers, education and training providers, and learners (Petersen, 2021). The NICE Framework attempts to define the TKSs in generic terms that can be applied to all organizations and are agile, flexible, interoperable, and modular (Petersen, 2021). The NICE Framework is comprised of seven categories of common cybersecurity functions which are broken down into 33 specialized areas that have defined Knowledge, Skills, and Abilities (KSAs) to complete defined tasks for that specialized area. Additionally, “Capability Indicators” for Entry, Intermediate, and Advanced roles across training, experiential learning, education, continuous learning, and credentials and certifications are defined. These items provide the building blocks for a Capable and Ready Cybersecurity Workforce (Figure 1).

![Figure 1: Building Blocks for a Capable and Ready Workforce (Newhouse, 2017)](image)

The National Security Agency’s (NSA) Cryptologic School manages the National Centers of Academic Excellence in Cybersecurity (NCAE-C). NCAE-C is supported by multiple federal partners to create and manage a collaborative cybersecurity educational program with community colleges, colleges, and universities that:

- Establish standards for cybersecurity curriculum and academic excellence,
• Includes competency development among students and faculty,
• Values community outreach and leadership in professional development,
• Integrates cybersecurity practice within the institution across academic disciplines, and
• Actively engages in solutions to challenges facing cybersecurity education (NCAEC, N.D.)

Academic institutions may be awarded one of three designations based on various criteria: Cyber Defense, Cyber Research, and Cyber Operations. These academic institutions align their curriculum map to learning outcomes that align with the NIST / NICE Framework. Additionally, NCAE-C requires that designated programs integrate a continuous improvement process to ensure that the curriculum evolves with the state of cybersecurity (Figure 2).

Figure 2: NCAE-C Program of Study (PoS) Evaluation Conceptual Model (NCAEC, 2021)

The Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS), Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC), and the International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8) formed a Joint Task Force (JTF)
to develop curriculum guidelines for post-secondary degree programs in cybersecurity. The JTF’s mission was:

- To develop comprehensive and flexible curricular guidance in cybersecurity education that will support future program development and associated educational efforts at the post-secondary level, and
- To produce a curricular volume that structures the cybersecurity discipline and provides guidance to institutions seeking to develop or modify a broad range of programs, concentrations, and/or courses rather than a prescriptive document to support a single program type (CSEC, 2017).

The resultant work identified eight knowledge areas of data security, software security, component security, connection security, system security, human security, organization security, and societal security. Additionally, the team identified cross-cutting concepts of confidentiality, integrity, availability, risk, adversarial thinking, and systems thinking. This body of knowledge was then viewed through the disciplinary lenses of information technology, information systems, computer science, computer engineering, software engineering, and other disciplines. This is captured in the CSEC thought model (Figure 3). Each of the knowledge areas is further defined by identifying knowledge area essentials and then providing the knowledge units and topics associated with the knowledge area.
Further, The ACM Committee for Computing Education in Community Colleges (CCECC) designed the Cybersecurity Curricular Guidance for Associate-Degree programs based on CSEC 2017 and influenced by the CAE-CD 2Y 2019 knowledge units, the NICE Cybersecurity Workforce Framework, and other relevant sources (CCECC, 2020). The curricular guidance guided how to use the guidelines focusing on conducting program reviews to update and create curriculum, facilitating program and course articulation, complying with government-sponsored frameworks, and interacting with local advisory boards (CCECC, 2020).

Finally, at the K-12 education level, Cyber.org published the national K-12 Cybersecurity Learning Standards focused on the key fundamentals of cybersecurity education including computing systems, digital citizenship, and security. TeachCyber’s High School Cybersecurity Curriculum Guidelines build upon these standards and were developed to accomplish the following goals:

- Set the parameters, directions, and standards for curriculum policy and practice,
- Provide a means for organizing and managing content systematically,
• Enable educators to effectively plan properly sequenced activities to provide learning opportunities targeting desired learning outcomes, and
• Ensure that students develop a base of knowledge, skills, attitudes, beliefs, and values to function successfully in cybersecurity college programs and careers (Dark, N.D.).

These guidelines identify eight “Big Ideas” like ACM’s Knowledge Areas. The “Big Ideas” include ethics, establishing trust, ubiquitous connectivity, data security, system security, adversarial thinking, risk, and implications (Dark, 2021). For each idea there are several essential questions associated with them. Based on these questions, the idea is broken down into enduring understanding, associated learning objectives, and essential knowledge statements. This formulation is depicted in Figure 4.

**Big Idea #1 – Ethics**
Cybersecurity has broad implications. Ethical reflection and judgement are required to make decisions about the trade-offs between the benefits and harms. Whether a system’s design or the use of the system constitutes a benefit or harm depends on the ethical duties and interests of both the designer and user. Designers and users can have differing interests when it comes to deciding what is worth protecting and which cybersecurity resource investments are justified to achieve that protection. All cybersecurity exists within a context of social, organizational, and personal values; these values undergird beliefs about right and wrong. In this course, students will have the opportunity to evaluate the ethical implications among all stakeholders.

**Essential Questions:**
- What is an ethical way to disclose vulnerabilities?
- How do values shape the security considerations of designers?
- How do values shape the security considerations of users?
- How do core societal values shape the security considerations in what is allowed or encouraged to be created?

<table>
<thead>
<tr>
<th>Enduring Understanding</th>
<th>Learning Objectives</th>
<th>Essential Knowledge Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1: Social goals reflect the foundational values held by society; these core societal values are reflected in cybersecurity choices.</td>
<td>1.1.1: Students will analyze online and offline behaviors in societies, i.e., themselves, peers, families, communities, and countries, and deduce the values that govern these behaviors.</td>
<td>1.1.1a: Societies are groups of individuals characterized by common interests/values that are perpetuated by persistent social interaction. 1.1.1b: Cybersecurity ethics is an expression of values by the designers and users.</td>
</tr>
</tbody>
</table>

**Figure 4: Big Idea #1 Ethics: High School Cybersecurity Curriculum Guidelines (Dark, 2021)**
2.3 Curriculum

The National Cybersecurity Training and Education (NCyTE) Center aims to advance cybersecurity education in the U.S. by investing in technological innovation, resources, professional development, and tools to support faculty, community colleges, and the workforce pipeline of tomorrow (About NCyTE, 2021). NCyTE provides resources for faculty, industry, and centers of academic excellence. Additionally, NCyTE provides cybersecurity curriculum consisting of dozens of modules across a variety of topics including Advanced Placement Computer Science Principles, Cybersecurity, Cyber Intelligence Curriculum, Critical Infrastructure Security & Resilience (CISR), Critical Infrastructure Cybersecurity, Applied Cryptography, Cyber Threats & Counter Measures, Responsible Software Development, Secure Scripting, Cybersecurity and Society, Cybersecurity Principles, and Securing Data From Risk (Cybersecurity Curriculum, 2021). NCyTE supplements this content by providing webinar series, workshops, and resources to run camps and other activities.

Similarly, Cyber.org’s goal is to empower educators as they prepare the next generation to succeed in the cybersecurity workforce and ensure that every K-12 student receives foundational and technical cybersecurity knowledge and skills (Cyber.org, 2021). Cyber.org released the first national K-12 cybersecurity learning standards focused on computing systems, digital citizenship, and security. These core themes are further broken down as depicted in Figure 5.
Cyber.org has thousands of hours of curriculum broken down by grade level across career and technical education, computer science, cybersecurity, engineering, humanities, math, robotics and coding, and science. Additionally, Cyber.org provides professional development to empower educators. Most recently, Cyber.org has released a comprehensive year-long course to support educators teaching high school cybersecurity supported by a no-cost virtual environment to practice the skills and activities in the curriculum.

Two additional resources for obtaining and sharing resources and curriculum are the Centers of Academic Excellence in Cybersecurity Resource Directory (CARD) (CARD, 2021) and the Cybersecurity Labs and Resource Knowledge Base (CLARK) (CLARK, 2021) to support educational institutions. CARD is a general resource directory that contains reports, grant deliverables, conference resources, competition frameworks, workshops and materials, and additional resources to support labs and summer camps. CLARK is focused on the development and sharing of cybersecurity curricula. Content is broken down by topic (22 topic areas), education level (Elementary-, Middle-, High-School, Undergraduate, Graduate, Post-Graduate,
Community College, and Training), and length (Nanomodule – 1 hour or less, Micromodule – 1 – 4 Hours, Module – 4 – 10 Hours, Unit – Over 10 Hours, Course – 15 Weeks) (CLARK, 2021).

2.4 Current Solutions

The developed curriculum and support by the U.S. government appear to support solving the cybersecurity education and workforce development problem. NIST / NICE, Cyber.org, and NCAE-C outline standards; TeachCyber outlines high school cybersecurity guidelines; and NCyTE, Cyber.org, CARD, and CLARK provide hundreds of hours of curriculum, content, workshops, and webinars to empower educators. Despite this, cybersecurity education and workforce development problems continue to exist. There are a few reasons for this. First, focused cybersecurity education and training mostly begins at the collegiate level and is siloed. Second, industry does not know what KSAs they need for the roles they are trying to fill. This is evident in job ads where skills, position levels, and pay are incongruent. Finally, the movement of cybersecurity education into the K-12 space is required.

Cybersecurity seemingly must be implemented at birth considering that internet-connected toys and devices enter children’s lives at a very young age. This section outlines previous work that addresses Cyber-Safety, Cyber-Education, and Cyber-Skills designed to improve the capabilities of the cybersecurity workforce and reduce risk.

2.4.a Cyber-Safety

Cyber-Safety initiatives can reduce the nation’s susceptibility to cybercrime and reduce risk. Cybercriminals typically prey on the weakest or most vulnerable; therefore, steps must be taken to educate and prepare those systems and populations at the greatest risk. Cyber-Safety applies to everyone. People are introduced to technology at different points in their lives and their fluency with technology depends on many factors. Cyber-safety should be introduced at a
young age considering technology will be part of their entire lives. Children are taught how to
safely navigate their world from a young age. This includes how to safely cross the street, not
touching sharp or hot objects, wearing protective devices like helmets and seat belts, fire safety,
stranger safety, and water safety. The research, content, and application of cyber-safety for
children birth to 5 years remain under-researched and limited in practice (Edwards, 2021).
Additionally, the long-term impacts of identity theft on this population may not be understood
for years.

Similarly, the elderly population, those aged 65 years or more, are at increased risk.
Cybercrime against the elderly fits into two general categories of fraud committed by strangers
targeting investments, charity contributions, loans and mortgages, and financial exploitation by
relatives and caregivers (Arfi, 2013). According to the FBI (Munanga, 2019), older adults are
prime candidates for these crimes due to their credit history and when cognitive decline
necessitates the need for others to manage their finances. This cohort typically lacks the
familiarity with technology that other generations have. Additionally, they are less likely to be
cognizant of cybersecurity threats and lack the experience to identify fraud in the digital space.
The Center for Internet Security (Aliperti, 2021), Cyber Patriot CyberGenerations Program
(CyberPatriot 2022), the CISA (CISA, 2022), and various industry and government partners
offer training and resources to support the elderly. Despite the increased awareness, training, and
available resources; the financial damage for seniors is estimated at $1.68 billion annually
(Abbate, 2021).

2.4.b Cyber-Education

As previously mentioned, there are seven common cybersecurity functions and 33
specialized areas as defined in the NICE Framework. These areas span from the non-technical to
the deeply technical. Individuals from all backgrounds leverage digital resources during daily life. Thus, cybersecurity education content must be tailored to the audience. Research conducted at Southeastern Louisiana University determined that survey participants not in a technology-focused major are at a disadvantage when it comes to general cybersecurity knowledge and privacy practices (McNulty, 2021).

Similarly, cybersecurity education must be integrated into all education levels. The curriculum must be tailored to be digestible and applicable for each age and education level. This requires a multi-level, multi-discipline approach that provides a level of cybersecurity education that is appropriate for an individual’s role in society as depicted in Figure 6.

![Figure 6: Multi-Level, Multi-Discipline Cyber Education Approach (Sobiesk, 2015)](image)

Additionally, cybersecurity educational programs vary in content, application, breadth and depth, and integrated labs with hands-on learning. The work of NICE, NCyTE, Cyber.org, and others seeks to ensure that graduates at various levels have the tangible skills necessary to secure and thrive in the cybersecurity profession. There are approximately 80 CAE-R, 23 CAE-CO, and over 200 CAE-CD designated schools (CAE, 2021). These schools meet or exceed the
requirements set by the National Security Agency and are reviewed by peer institutions to ensure consistency and quality across schools.

Cybersecurity education programs focusing on high school students are being developed. Regions Investing in the Next Generation (RING) is an online high school cybersecurity course that offers content for students and schools without existing cybersecurity programs. RING officially launched in 2022 allowing students to achieve high school credit in participating states (RING, 2022). RING also provides networking and professional development through the RING student organization. Additionally, Cyber.org facilitated collaboration among key stakeholders to develop and publish a set of K-12 cybersecurity learning standards centered on computing systems, digital citizenship, and security to ensure that students have a foundational understanding of cybersecurity and the skills and knowledge to pursue cybersecurity careers (Cyber.org, 2022). These standards led to the development of cybersecurity education curriculum and a cybersecurity range to support cybersecurity learning.

2.4.d Cyber-Skills

People starting their cybersecurity careers have three primary methods for developing skills necessary to increase employability. These are learning skills through formal, non-formal, and informal learning activities. Non-formal and informal activities include self-study or other experiential learning and completing industry certifications, or formal learning by gaining a related degree (Marquardson, 2018). This section focuses on the complementary skill development of certifications, On-the-Job Training (OJT), internships, apprenticeships, and experiential learning.
2.4.d.i Certifications

Research indicates that certifications are important since they build confidence in cybersecurity professionals, validate their level of knowledge and skills versus untrained employees, and can execute their assigned tasks more consistently (James, 2019). Since 1989, Information Technology (IT) certifications have been introduced to reinforce and assess individuals or groups (Jarocki, 2019). Certifications are generally broken down into vendor-neutral and vendor-specific. Certification vendors factor in the current threat landscape, changing technologies, workforce needs, industry standards, and government regulations to develop and maintain the certifications. These factors are depicted in Figure 7.

![Figure 7: Factors Impacting the Maintenance of Cybersecurity Certifications (Knapp, 2017)](image)

There are hundreds of cybersecurity certifications provided by many organizations. These include, but are not limited to, the Computing Technology Industry Association (CompTIA), the International Council of Electronic Commerce Consultants (EC-Council), Global Information Assurance Certification (GIAC), ISACA, and the International Information

2.4.d.ii On-the-Job-Training / Apprenticeships / Internships / Experiential Learning

Cybersecurity degree programs obtain a competitive advantage based on the amount of “hands-on” content within the curriculum considering industry requires a significant amount of skills-based training (Glantz, 2021). Complementing the “hands-on” content embedded into education programs and certifications is On-the-Job Training (OJT), internships, apprenticeships, and experiential learning. Internships and apprenticeships allow potential employees to gain, develop, and refine their cybersecurity skills while providing insight into the career field. Access and value to these opportunities vary. Figure 8 outlines the key differences between these two opportunities.

![Table of Internship and Apprenticeship Differences](image)

Figure 8: Internship and Apprenticeship Differences (Stoker, 2021)
Although the experiences vary, the results are positive considering those that complete at least one internship receive 16% more job offers than those who don’t and 94% of individuals that complete an apprenticeship program retain employment (Goin, 2021). Additionally, apprenticeships are becoming a growing initiative supported by the government. The National Initiative for Cybersecurity Education (NICE) Cybersecurity Apprenticeship Program Finder was a tool developed to support future cybersecurity professionals through paid work experience and work-based learning, classroom instruction, mentoring, and a nationally- or state-recognized credential upon completion of the program (NIST NICE, 2022). This effort aligns with the Cybersecurity Apprenticeship Sprint led by the Department of Labor, the White House, the U.S. Department of Commerce, and other federal agencies. The results of this 120-day initiative include:

- 194 cybersecurity registered apprenticeship programs approved or under development,
- Program sponsors added 120 cybersecurity-related occupations to pre-existing and newly registered apprenticeship programs,
- 7,000 apprentices hired,
- Major organizations like IBM, CompTIA, and the Department of Defense (DoD) expanding their programs and Boeing, Cisco Systems, McDonald's, Department of Veterans Affairs, and more launched new programs, and
- Over 2,000 organizations and career seekers expressed interest in learning more about the registered apprenticeship program (The White House, 2022).

Experiential learning in the form of self-study, participating in summer camps, and participating in “capture-the-flag” competitions can augment other skill development opportunities. For example, the Air Force Association (AFA) sponsored CyberPatriot program
has evolved from a defense-based cybersecurity competition to include a curriculum to support the elderly (Cybergenerations), educators (Elementary School Cyber Education Initiative (ESCEI)), and an information campaign through their CyberPatriot Literature Series. The CyberPatriot National Youth Cyber Defense competition challenges teams of high school and middle school students to find and fix cybersecurity vulnerabilities in virtual operating systems (CyberPatriot, 2021). Alternatively, the GenCyber program provides cybersecurity experience for students and teachers at the secondary education level. GenCyber focuses on:

- Increasing awareness of K-12 cybersecurity content and career opportunities,
- Increase student diversity in cybersecurity college and career readiness pathways, and
- Facilitate teacher readiness within a teacher learning community (GenCyber, 2022).

Finally, the National Cyber League (NCL) bridges the gap between high school and college students by providing a performance-based, learning-centered cybersecurity competition providing practical cybersecurity challenges competitors are likely to face in the workplace (NCL, 2021). Additional learning activities include the TryHackMe (TryHackMe, 2021) and HacktheBox (HTB, 2021) platforms for gaining hands-on cybersecurity skills as another option to develop cybersecurity skills.

### 2.5 Literature Review Synopsis

The literature identifies many cybersecurity education initiatives at various education levels. The various organizations and documents outlined in this chapter provide answers to different aspects of cybersecurity education. Despite the variety of disparate initiatives, there lacks a formalized understanding of cybersecurity education programs at secondary education institutions. Additionally, a single unifying framework to support secondary education institutions for cybersecurity education doesn’t exist. Table 1 depicts the different organizations
and documents discussed and the aspects of cybersecurity education that they address. The categories of Knowledge, Skills, Abilities, and Tasks (KSATs), Standards, Guidelines, Learning Objectives, Curriculum / Content, and Applicability Level are used.

<table>
<thead>
<tr>
<th>Organization</th>
<th>KSATs</th>
<th>Standards</th>
<th>Guidelines</th>
<th>Learning Objectives</th>
<th>Curriculum / Content</th>
<th>Applicability Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST / NICE</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Workforce</td>
</tr>
<tr>
<td>NCAE-C</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>Post-Secondary</td>
</tr>
<tr>
<td>ACM</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>Post-Secondary</td>
</tr>
<tr>
<td>Cyber.org</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>Secondary</td>
</tr>
<tr>
<td>Teach Cyber</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>Secondary</td>
</tr>
<tr>
<td>RING</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>Secondary</td>
</tr>
<tr>
<td>CLARK / CARD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>Various</td>
</tr>
</tbody>
</table>

*Table 1: Organization Crosswalk*
CHAPTER 3

Research Methodology

The purpose of this study is to develop program profiles of cybersecurity education programs established at secondary education institutions in Arizona. These program profiles will identify the elements, requirements, and motivations for developing said cybersecurity programs. A secondary outcome of the study will be to develop an initial comprehensive cybersecurity education framework for secondary education institutions based on the elements identified in the case study that can be adopted by various school districts throughout Arizona. The framework will incorporate formal, non-formal, and informal learning activities. The study objectives are to develop cybersecurity education program profiles of existing cybersecurity programs in Arizona, develop a CyberEducation-by-Design framework, and initially evaluate the CyberEducation-by-Design Framework by interviewing stakeholders that participated in the case study. The output of this study addresses the underlying problem of the lack of cybersecurity professionals needed to fill the growing industry demand by introducing comprehensive cybersecurity education at secondary education institutions. The program profiles should provide secondary education institutions with a template for developing cybersecurity programs at that level. The proposed framework should guide secondary education institutions’ ability to develop entry-level cybersecurity professionals with the pre-requisite qualifications, knowledge, skills, and abilities desired by employers thereby reducing the cybersecurity workforce shortage. Additionally, the proposed framework should be designed with pathways to employment, military service, trade or certification programs, or post-secondary education in pursuit of their ultimate education and career goals. The framework will be designed to facilitate cybersecurity education and workforce
development at the secondary education level (9-12 grade) within Arizona. Further, the components of the model should be modular and scalable. Modular meaning that schools should be able to adopt cybersecurity education components that support their specific institution. Scalable in that it meets the requirements of the school, the districts, and the state. This chapter will explore the selected research methodology, the research design approach, the reasons for selecting this methodology, and its validity.

3.1 Research Approach

This work will utilize case study research. Yin (2003) defines case study research as “an empirical inquiry that investigates a contemporary phenomenon within its real-life context when the boundaries between phenomenon and context are evidence…and it relies on multiple sources of evidence.” Additionally, Wieringa (2014) defines an observational case study as “a study of a real-world case without performing an intervention.” Case study research requires gathering data from multiple sources. According to Bekmamedova (2018), data collection techniques include interviews, observations, questionnaires, and relevant documents. This research will use three data collection techniques: review relevant documents, conduct interviews, and compile direct observations of the program. This data will be compiled into program profiles which will inform the development of the CyberEducation-by-Design Framework.

3.2 Context

Specifically for this research, the knowledge goal is to determine the elements of existing cybersecurity secondary education programs to develop program profiles. The improvement goal is to develop a comprehensive framework; the CyberEducation-by-Design Framework, for secondary education institutions seeking to start a cybersecurity education program. The
framework incorporates formal, non-formal, and informal learning activities to develop students with the KSAs to move on to the next stage of their professional journey and improve student success. CyberEducation-by-Design is a new framework within this discipline; however, traditional pedagogies, curriculum development processes, and existing content can be used to contribute to the design theory.

3.3 Research Design

The five components related to case studies identified by Yin (2003) will inform the research design for this research. The five components include:

1. A study’s questions.
2. Its propositions, if any.
3. Its unit(s) of analysis,
4. The logic linking the data to the propositions; and
5. The criteria for interpreting the findings.

3.3.a Study Questions

Yin (2003) suggests that the case study approach is most likely to use how and why questions which must be clarified within the study. For this research, publicly accessible data will be collected to establish the initial program profile. Questionnaires and interviews will be conducted to identify additional elements missing from the initial program profile and provide context on how the program was established, identify the personnel and resources available, identify challenges and opportunities in establishing the program, and determine future growth and initiatives of the programs. The results of the data collection will be used to complete the program profiles to answer the first research question. The interview will follow a semi-structured approach. Semi-structured interviews have the following characteristics:
• The interviewer and respondents engage in a formal interview.
• The interviewer develops and uses an ‘interview guide.’ This is a list of questions and topics that need to be covered during the conversation, usually in a particular order.
• The interviewer follows the guide but can follow topical trajectories in the conversation that may stray from the guide when he or she feels this is appropriate. (Cohen, 2006).

Additionally, Roberts (2020) provides two additional elements that apply to this research. The interview provides an open-ended, in-depth exploration of an aspect of life about which the interviewee has substantial experience, often combined with considerable insight (Roberts, 2020). The interview question can be evaluated to both a thematic and a dynamic dimension:

• Thematically about producing knowledge.
• Dynamically about the interpersonal relationship in the interview (Roberts, 2020).

The research will begin by reviewing publicly available information to fill in the pertinent data across six primary sections of the program profile including demographics, operations, formal learning, non-formal learning, informal learning, and pathways (Table 2). Interviews will provide additional context to complete the program profiles and identify the motivations for starting the cybersecurity education programs, the development process, the evolution of the program, challenges and opportunities, and goals and potential future initiatives.

The questions are outlined in the interview guide.

3.3. b Interview Questions

Interviewee Questionnaire

1. What is your current role or job title?
2. If applicable, what academic degrees do you hold?
3. If applicable, what industry certifications do you hold?
4. How many years of experience do you have in secondary education?

5. What courses have you taught at the secondary education level and how many years have you taught each course?

6. If applicable, how many years of experience do you have in industry work related to cybersecurity, information technology, computer science, or related fields?

7. What was your role in developing the cybersecurity education program at your institution?

8. If there is anyone else that you believe had input into the program and can provide insight into program development and operations, please provide them with my contact information and have them contact me.

Program Profile Questionnaire Questions

1. Describe the operational elements of the cybersecurity education program.

   a. Instructors (Education, Certifications, Years of Experience (Teaching / Industry), Courses Taught, Dual Enrollment Qualified (If so, What Courses)).

<table>
<thead>
<tr>
<th>Teacher</th>
<th>Education Level</th>
<th>Certifications</th>
<th>Years of Experience Teaching</th>
<th>Industry</th>
<th>Courses Taught</th>
<th>Dual Enrollment Qualified</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   b. Equipment (Type, Make, Model, Number, Cost)

<table>
<thead>
<tr>
<th>Equipment Type</th>
<th>Make</th>
<th>Model</th>
<th>Quantity</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2. Describe the formal learning activities. Formal learning is the type of learning that is intentional, organized, and structured. Formal learning opportunities are usually arranged by institutions. Often this type of learning is guided by a curriculum or other type of formal program.

   a. What courses are included in the cybersecurity program?
   b. What are the course descriptions for courses within the cybersecurity program?
   c. Can you provide the syllabi for the courses within the cybersecurity program?
   d. Is the course designated as dual enrollment?
   e. Did the course exist before the development of the cybersecurity program?

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Syllabus</th>
<th>Dual Enrollment</th>
<th>Pre-Existing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Interview Questions

1. What was the motivation for starting a cybersecurity education program at your institution?

2. Describe how the cybersecurity education program was developed at your institution.
   a. What standards, guidelines, or frameworks were used to develop the program?
   b. How were the courses selected for inclusion in the cybersecurity program at your institution?

3. Describe the operational elements of the cybersecurity education program.
   a. Instructors
      i. How are qualified teachers identified or hired to teach cybersecurity courses?
ii. If applicable, describe the challenges in finding qualified instructors for cybersecurity courses.

b. Equipment
   i. How was the equipment listed identified or determined to be needed to support the selected courses?
   ii. If applicable, describe the challenges in procuring the equipment necessary to support the selected courses.

c. Networks
   i. Describe the networks that students use for their cybersecurity curriculum and assignments.
   ii. If applicable, describe the challenges in operating on those networks.

d. Facilities
   i. What facilities are used by students in the cybersecurity program?
   ii. Are these facilities utilized by students outside the cybersecurity program and if so by what programs?
   iii. Describe the process for acquiring these facilities.
   iv. If applicable, describe the challenges in obtaining these facilities to support the selected courses.

4. Describe the formal learning activities. Formal learning is the type of learning that is intentional, organized, and structured. Formal learning opportunities are usually arranged by institutions. Often this type of learning is guided by a curriculum or other type of formal program.
   a. Why were these courses selected for inclusion in the program?
5. Describe the non-formal learning activities. Non-formal learning is a type of learning that may or may not be intentional or arranged by an institution, but is usually organized in some way, even if it is loosely organized. There is no form of credit granted in non-formal learning situations. Examples of non-formal learning activities include camps, certifications, internships, and apprenticeships.
   a. Based on the provided definition and examples, what non-formal learning activities are incorporated into the cybersecurity program?
   b. How do these activities support the cybersecurity program and cybersecurity students?

6. Describe the informal learning activities. Informal learning is a type of learning that is never organized. Rather than being guided by a rigid curriculum, it is often thought of as experiential and spontaneous. Examples of informal learning activities include clubs, competitions, self-study / ad-hoc learning, conferences, and industry events.
   a. Based on the provided definition and examples, what non-formal learning activities are incorporated into the cybersecurity program?
   b. How do these activities support the cybersecurity program and cybersecurity students?

7. Describe the pathways for students. Students have four primary options after graduating from secondary education: go directly into the workforce, join the military, enter a trade or certification program, or attend post-secondary education.
   a. How does the cybersecurity program prepare students for the various pathways outlined above?
b. How does the program track students upon graduation from the cybersecurity program?

Framework Evaluation Questions

1. Does the proposed framework integrate formal, non-formal, and informal learning activities adequately, and if not what should be integrated into the framework to make it more comprehensive?
   a. How would this have supported the development of the cybersecurity education program at the institution?

2. Describe how the inclusion of standards, guidelines, and curriculum would support the development of a cybersecurity education program.
   a. How would this have supported the development of the cybersecurity education program at the institution?

3. In what ways would the proposed framework have assisted in the development of a cybersecurity education program at the institution?

4. In what ways is the proposed framework lacking that should be included to support the development of cybersecurity education programs at the institution?

3.3.3 Cybersecurity Education Program Profile Draft

<table>
<thead>
<tr>
<th>Demographics</th>
<th>Section</th>
<th>Area</th>
<th>Specifics</th>
<th>Data</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enrollment</td>
<td></td>
<td>White</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hispanic / Latino</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Asian or Asian / Pacific Islander</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Black or African American</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>American Indian or Alaska Native</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 2: Draft Program Profile

#### 3.3.d Study Propositions

According to Yin (2003), each proposition directs attention to something that should be examined in the scope of the study. Based on a review of the literature about the current state of cybersecurity education at secondary education institutions, the following propositions can be formed.
Proposition 1: Evaluating current cybersecurity programs at secondary education institutions can identify elements needed to develop program profiles that can inform the development of a comprehensive cybersecurity education framework.

Proposition 2: Lack of a comprehensive cybersecurity education framework for cybersecurity education programs at secondary education institutions leads to incomplete, inconsistent, or inefficient development of cybersecurity education programs at the secondary education level.

Proposition 3: The evaluation of a proposed comprehensive cybersecurity education framework can be conducted by comparing to program profiles and conducting follow up interviews with case study participants.

3.3. e Unit of Analysis

The unit of analysis for a “case” study can be an individual(s) or an event or entity. According to Yin (2003), case studies have been done about decisions, programs, the implementation process, and organizational change. In this study, a case is defined as a cybersecurity education program at a secondary education institution. School selection is based on school location, comprehensiveness of the program at the school, proximity to auxiliary elements to be evaluated, and accessibility to data for the resident programs. Case 1 (Basha High School’s Cybersecurity Education Program) and Case 2 (Chandler High School’s Cybersecurity Education Program) are schools within Chandler Unified School District in Chandler, Arizona. These schools are in Maricopa County. Two stakeholder groups will be interviewed during this study. Group one will consist of individuals that were directly involved in the development of the cybersecurity program at the secondary education institution. Group two will consist of
individuals that had input into the cybersecurity program or teach within the cybersecurity program.

The following information is provided for the context of the area of study. Maricopa County is the largest county in Arizona with a population of approximately 4.5 million, making it the fourth largest county in the United States (World Population Review, 2022). General demographics for Maricopa County include 54% White (Non-Hispanic), 25% White (Hispanic), 5.5% Black or African American, 4.6% Other (Hispanic), 4% Asian; ~253,000 veterans; $68,649 Median Household Income; 13.8% categorized as poverty status (Maricopa County, 2022).

Community Colleges play an important role in post-secondary education within Arizona. These two-year schools enable students to gain education, training, and experience while meeting the needs of local industries. Maricopa County has a community college system comprised of 10 community colleges that can support student transition and success. Three community colleges, Glendale Community College (GCC), Estrella Mountain Community College (EMCC), and Chandler Gilbert Community College (CGCC) have dedicated 2-year cybersecurity degrees. Glendale Community College and Estrella Mountain Community College are designated National Centers of Academic Excellence in Cybersecurity (NCAE-C). Each of these community colleges has articulated transfer pathways to the University of Arizona’s (UA) NCAE in Cyber Operations program. In addition to UA, there are three 4-year NCAE-C designated cybersecurity programs within Maricopa County: Grand Canyon University (GCU), University of Advancing Technology (UAT), and Embry Riddle Aeronautical University (ERAU). These institutions can be pathways and support for cybersecurity programs at secondary education institutions.
3.3.f Logic Linking the Data to the Propositions

The propositions were developed previously in section 3.3.3. The interview questions and subsequent development of the program profile for each school will be compared to ensure the completeness of the profile and the propositions for secondary education institutions. Additionally, the data from the initial interviews and program profiles will inform the development of the cybersecurity education framework addressing proposition two. Further, follow-up interviews will provide initial insight into how the proposed framework would have benefited or not benefited the development of the cybersecurity programs at those institutions addressing proposition three.

3.3.g Criteria for Interpreting the Findings

Yin (2003) describes a case study from Campbell which did not do any statistical test, nor would a statistical test be possible due to each obtained data point being a single number. Given the nature of this case study, statistical analysis would not be appropriate. Therefore, analogic inference will be used. Analogical reasoning provides the ability to determine similarities and to make inferences from one situation to another (Colhoun, 2009). This method is appropriate considering that public K-12 schools share a similar architecture, follow state testing standards, and generally follow similar operational aspects. The intended scope of the generalization will be that program profiles can be developed for cybersecurity education programs throughout the state and the U.S. Similarly, the proposed CyberEducation-by-Design framework could be applied to schools throughout Arizona and the U.S. high schools in different districts may have differences which may introduce limitations to this generalization and those differences must be understood before applying the framework outside the test school district.
CHAPTER 4

Analysis, Results, and Discussion

This study can be used to begin discussions at secondary institutions throughout Arizona and beyond. The results can inform practice, research, and theory within the cybersecurity education space. This chapter will discuss the case studies and associated data collection used to develop the program profiles. The program profile elements were used to develop the initial CyberEducation-by-Design framework. Additional elements were incorporated into the framework that were not part of the program profiles due to their availability after the case study programs were developed. Finally, the CyberEducation-by-Design framework was presented to case study participants to get their initial feedback on the framework, its comprehensiveness, and perceived value to institutions considering implementing a cybersecurity education program.

4.1 Program Profiles

The program profiles provide insight into the cybersecurity programs at secondary education institutions within the Chandler Unified School District. The insight can identify personnel, resources, challenges, and opportunities for other schools to adopt the proposed framework.

Chandler, Arizona is in Maricopa County, Arizona. Table 3 provides city demographics in which Basha High School and Chandler High School are located.

<table>
<thead>
<tr>
<th>Chandler, Arizona Demographics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Population</td>
</tr>
<tr>
<td>Median Income</td>
</tr>
<tr>
<td>Poverty Rate</td>
</tr>
<tr>
<td>Unemployment Rate</td>
</tr>
</tbody>
</table>
Race and Hispanic Origin

<table>
<thead>
<tr>
<th>Race and Hispanic Origin</th>
<th>White not Hispanic or Latino: 56.4%</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hispanic or Latino: 21.5%</td>
</tr>
<tr>
<td></td>
<td>Asian: 10.9%</td>
</tr>
<tr>
<td></td>
<td>Black or African American: 5.6%</td>
</tr>
<tr>
<td></td>
<td>American Indian and Alaska Native: 1.7%</td>
</tr>
<tr>
<td></td>
<td>Native Hawaiian/Other Pacific Islander: .2%</td>
</tr>
<tr>
<td></td>
<td>Other: 2.7%</td>
</tr>
</tbody>
</table>

Table 3: Chandler AZ Demographics (Census, 2022)

4.1.a Chandler Unified School District

Chandler Unified School District is located at 1525 W. Frye Rd., Chandler, AZ 85249 whose website is [https://www.cusd80.com/](https://www.cusd80.com/). Table 4 provides demographics for the district.

<table>
<thead>
<tr>
<th>Chandler Unified School District Demographics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student Population</td>
</tr>
<tr>
<td>Schools</td>
</tr>
<tr>
<td>Minority Enrollment</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enrollment by Diversity</th>
</tr>
</thead>
<tbody>
<tr>
<td>White not Hispanic or Latino: 49.8%</td>
</tr>
<tr>
<td>Hispanic or Latino: 28.6%</td>
</tr>
<tr>
<td>Asian: 9.8%</td>
</tr>
<tr>
<td>Black or African American: 5.2%</td>
</tr>
<tr>
<td>American Indian and Alaska Native: 1.3%</td>
</tr>
<tr>
<td>Native Hawaiian/Other Pacific Islander: .3%</td>
</tr>
<tr>
<td>Other: 5%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Teachers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student – Teacher Ratio: 18.1</td>
</tr>
<tr>
<td>Percentage of Teachers Certified: 100%</td>
</tr>
<tr>
<td>3 or more years of experience: 92.2%</td>
</tr>
<tr>
<td>Full-time counselors: 77</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Revenue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue: $445,501,000</td>
</tr>
<tr>
<td>Revenue by Source: 48.2% Local, 47.3% State, 4.4% Federal</td>
</tr>
<tr>
<td>Revenue per Student: $9,894</td>
</tr>
<tr>
<td>Expenses per Student: $7,995</td>
</tr>
</tbody>
</table>

Table 4: Chandler Unified District Demographics (US News, 2019)

4.1.b Basha High School

Basha High School is located at 5990 S. Val Vista Dr, Chandler, AZ 85249 whose website is [https://www.cusd80.com/BHS](https://www.cusd80.com/BHS). Table 5 provides the overall demographics for the school.
### Basha High School Overall Demographics

<table>
<thead>
<tr>
<th>Student Population</th>
<th>2,604 (6-12 Grade)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minority Enrollment</td>
<td>34.4%</td>
</tr>
</tbody>
</table>

| Enrollment by Diversity | White not Hispanic or Latino: 65.6%  
|                        | Hispanic or Latino: 17.1%  
|                        | Asian: 7.8%  
|                        | Black or African American: 4%  
|                        | American Indian and Alaska Native: 1.6%  
|                        | Native Hawaiian/Other Pacific Islander: .3%  
|                        | Other: 3.6%  |

| Teachers | Full-time Teachers: 120  
|          | Student – Teacher Ratio: 22  
|          | Percentage of Teachers Certified: 100%  
|          | 3 or more years of experience: 93.7%  
|          | Full-time counselors: 6  |

| Test Scores | Math Proficiency: 79% (5th in State)  
|            | Reading Proficiency: 77% (3rd in State)  |

*Table 5: Basha High School General Demographics (Basha, 2021)*

#### 4.1.b.i Basha Program Profile Analysis

The entirety of the Basha High School Program Profile can be found in Appendix J. This section will highlight some of the important data collected for the program at this school. The first academic year of the program was 2019 – 2020. The program began with 60 students and there are currently 154 students in the program as of the 2022 – 2023 academic year. The detailed breakdown of students can be found in Figure 9. The cybersecurity program graduated one student in 2020, one student in 2021, two students in 2022, and will graduate 16 students in 2023. Figure 10 depicts the graduates and their chosen pathway post-graduation. Pathway data for 2023 graduates were not available at the time of this study.
Student diversity within Basha High School’s cybersecurity program is like the overall school demographics with 40.3% minority enrollment. Additionally, approximately 11% of students are female. These demographics represent higher diversity than other programs nationally; however, 11% of students identifying as female represent a lower percentage.
nationally. Demographic specifics and the comparison between Basha High School and the cybersecurity program are outlined in Figure 11.

Figure 11: Basha High School and Cybersecurity Program Demographics

The operational aspects of the cybersecurity program consist of personnel, equipment, network, and facilities. The program is primarily supported by three Full Time Equivalent (FTE) teachers. The Basha High School program director is considered an FTE; however, their primary responsibility is overseeing the cybersecurity program. Despite this, they were required to teach courses due to another full-time employee quitting early in the 1st quarter. This singular example is representative of the national shortage of cybersecurity teachers at all academic levels. The itemized initial equipment list for year one operations is in Appendix J. Initial startup costs were approximately $32,000. This is approximately $3,500 higher than Chandler High School’s program due to the inclusion of Cisco networking equipment. Additionally, the program required a separate network from the school district-provided network. The isolated network was installed in the cybersecurity classrooms and lab spaces to allow access to websites and resources to facilitate learning objectives that would be blocked on the district network. This isolation also
required separate hardware due to restrictions on district-provided equipment. Finally, the program has four dedicated learning areas. There are three general-purpose classrooms and one Career and Technical Education (CTE) lab. The CTE lab has a larger footprint consisting of teaching space and a space for hands-on activities and equipment storage.

Basha High School’s cybersecurity program’s formal learning activities were modeled after the established pathway between Chandler Gilbert Community College (GCCC) and the University of Arizona (UA). Developing the program had an initial goal of providing a seamless pathway from the high school, through the community college, to the university. The complete cybersecurity program partnership among the three institutions can be found in Appendix L. The courses within CGCC’s cybersecurity program were analyzed to identify which courses would fit into Basha High School’s cybersecurity program and articulation and pathways for students, meet dual-enrollment requirements, and align with existing Arizona CTE technical standards for network security identified as 11.1999.00. These standards are provided in Appendix M.

Ten courses were identified for inclusion into the program: Introduction to Computer Systems, Hardware and Software Configuration and Support (A), Hardware and Software Configuration and Support (B), Introduction to LAN and Security Fundamentals (A), Introduction to LAN and Security Fundamentals (B), Linux OS, Advanced Linux, Information Security Fundamentals, Ethics in Information Technology, and Python. The descriptions and syllabi for each course are outlined in the Basha High School cybersecurity program profile in Appendix J. Each of the ten courses allows dual enrollment. Although the courses were offered at CGCC before Basha High School’s program development, all educational requirements for the ten courses had to be created before delivery.
Additionally, Basha High School is a Cisco Networking Academy. This provides access to curriculum and teaching resources, equipment and software, professional development opportunities, and help students access job opportunities (Cisco, 2023). Further, the program leverages content, assessments, and labs from Cisco, TestOut, and Cengage to meet formal learning objectives. The course alignment and costs of these materials are outlined in Table 6. The program used RedHat Linux since program inception; however, due to changing requirements, the program will switch to Cisco curated content beginning in the 2023 – 2024 school year.

<table>
<thead>
<tr>
<th>Course</th>
<th>Company</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYB 240A / CNT 140 – Intro to LAN &amp; Security Fundamentals</td>
<td>Cisco</td>
<td>* Free Courseware</td>
</tr>
<tr>
<td>CYB 240B / CNT 150 – Intro to LAN &amp; Security Fundamentals</td>
<td>Cisco</td>
<td>* Free Courseware</td>
</tr>
<tr>
<td>CYB 300A / CIS 126DL – Linux OS</td>
<td>Cisco</td>
<td>$30 per student lab fee</td>
</tr>
<tr>
<td>CYB 300B / CIS 238DL – Advanced Linux</td>
<td>Cisco</td>
<td>$30 per student lab fee</td>
</tr>
<tr>
<td>CYB 400A / CIS 110 – Information Security Fundamentals</td>
<td>TestOut</td>
<td>$2,900 per year (50 user license)</td>
</tr>
<tr>
<td>CYB 400B / CIS 111 – Ethics in Information Technology</td>
<td>Cengage</td>
<td>$4,620 for Print Student Edition + 6 years access to online platform MindTap x 40 (price includes shipping and processing)</td>
</tr>
<tr>
<td>CYB 130 / CIS 156 – Python</td>
<td>Cisco</td>
<td>* Free Courseware</td>
</tr>
</tbody>
</table>

* Must be member of Western Academy Support & Training Center – WATSC (~$500 per year)

Table 6: Formal Learning Activity Materials and Fees

Non-formal learning activities include camps, certifications, internships, and externships. AZ Cyber Initiative and CyberPatriot are the cybersecurity-specific camps currently offered as part of Basha’s cybersecurity program. AZ Cyber Initiative is a multifaceted program offering scholarships, mentorship, internships, and cybersecurity boot camps. Scholarships provide financial assistance for high school students pursuing degrees or professional certifications in
cybersecurity-related fields or cybersecurity-related careers in the U. S. military. The mentorship program “connects high school students with qualified professionals to gain unique insights and important tools to help them find greater success (AZ Cyber Mentorship, 2023).” Paid internship opportunities are provided to students who complete the associated boot camp which will be discussed next. These internship opportunities place students with companies and professionals to serve as cyber consultants for small businesses. Finally, AZ Cyber Initiative provides camps to high school students and teachers. Each boot camp is a weeklong course that provides students with knowledge, hands-on activities, career development, and career exploration. The teacher boot camp prepares teachers to integrate content into existing courses and develop cybersecurity courses or programs. The CyberPatriot program provides multiple resources for middle and high school students. Basha High School began offering CyberPatriot camps in August of 2022. CyberPatriot offers a standard camp consisting of an introduction to CyberPatriot, an introduction to virtual machines, cyber ethics, Windows 10 and Ubuntu 18 Operating Systems. Additionally, an advanced camp offers cyber ethics, Windows 10 and Ubuntu 18 Operating Systems focusing on advanced skills and system administrator tasks and provides Cisco NetAcad access. Both camps offer a competition day to compete against other camps nationally.

A detailed discussion of the certifications integrated into Basha High School’s cybersecurity program is outside the scope of the study. Program curriculum aligns with or introduces concepts for A+, ITF+, Linux+, Security Pro, Security+, and Python Certified Entry-Level Program (PCEP) certifications. Certification allows high school students to be more employable and validate a foundational level of proficiency in several IT and cybersecurity work roles. For example, A+ aligns with Information Assurance Technical (IAT) I and Security+
aligns with Information Assurance Manager (IAM) I Department of Defense (DoD) approved baseline certifications (8570 Baseline Certifications, 2023).

Basha High School has partnered with several partners to provide students the opportunity to participate in internships and externships. The partnership with Open Source Integrators allows students to work with teams of open source Enterprise Resource Planning (ERP) professionals. The partnership with ElevateEd AZ provides externship opportunities. ElevateEd AZ is focused on aligning education to workforce learning paths. This initiative prepares students for college and careers by partnering with education, business, and community. The program specifically focuses on creating opportunities for high-wage, high-demand pathways which include Information Technology and Cybersecurity. Externships provide participants with a stipend upon completion of the program. The weeklong externship program consists of multiple sessions on technology-related topics, career pathways, required skills, and current events. Additionally, students participate in team-based projects and job preparation, and professional development sessions.

Informal learning activities include clubs, competitions, self-study and ad-hoc learning, conferences, and industry events. Basha High School’s cybersecurity program integrates multiple informal learning activities for students. As part of their overall CTE program, The Future Business Leaders of America (FBLA) and Family, Career, and Community Leaders of America (FCCLA) prepare students to become community-minded business leaders. FCCLA is an example of a student club. Additionally, Basha High School’s cybersecurity program offers students the opportunity to compete in the CyberPatriot competition and National Cyber League (NCL). CyberPatriot is typically held during the fall semester and NCL is held in the spring allowing students to compete throughout the school year. CyberPatriot competitions consist of a
network security challenge and a Cisco networking challenge. Teams compete over six hours. Whereas CyberPatriot focuses on network defense, National Cyber League is a comprehensive competition including Open Source Intelligence (OSI), cryptography, password cracking, log analysis, network traffic analysis, forensics, web application exploitation, scanning, and enumeration and exploitation (NCL Categories, 2023). Additionally, the Basha cybersecurity program set up a tour of the PhoenixNAP Data Center providing insight into one aspect of the career field. Finally, self-study and ad-hoc learning and conferences are not coordinated through the program but advertised and encouraged. Teachers and students participated in CactusCon a Phoenix-based cybersecurity conference, Women in Cybersecurity (WiCys), NICE K-12 Conference’s student signing day, and Embry Riddle Aeronautical Engineering cyber day.

Pathways become part of a future-focused program. Preparing students for post-secondary education, trade schools and certification training, military service, or the workforce provide options and opportunities. As previously mentioned, the formal learning activities were designed with pathways in mind. Specifically, this is the partnership with CGCC and UA. These designed pathways do not limit student opportunities for other post-secondary opportunities. Alternatively, students can pursue certification and workforce opportunities through Advanced Business Learning (ABL). ABL is a state-licensed school providing concurrent, subsequent, or alternative learning paths to develop cybersecurity knowledge and skills and obtain industry certifications. Specific cybersecurity-related training provided by ABL includes cybersecurity training aligned with DoD 8140 requirements, access to a cyber practice range, Risk Management Framework (RMF), and certification training for A+, Network+, Security+, Certified Ethical Hacker (CEH), and Certified Information Systems Security Professional (CISSP). Basha’s cybersecurity program partners with the school’s Junior Reserve Officer
Training Corps (JROTC) program. JROTC provides exposure to military service. Additionally, the school offers the Armed Services Vocational Aptitude Battery (ASVAB) to students during the fall semester. This provides the opportunity for career exploration and provides an initial starting point for enlisting in the military service. Finally, as an anecdotal example of direct to workforce pathway options, one of the first program cohort graduates was offered employment with Kelly Technologies.

4.1.c Chandler High School

Chandler Unified School District is located at 350 N. Arizona Ave., Chandler, AZ 85225 whose website is [https://www.cusd80.com/chs](https://www.cusd80.com/chs). Table 7 provides demographics for the school.

<table>
<thead>
<tr>
<th>Chandler High School Overall Demographics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student Population</td>
</tr>
<tr>
<td>Minority Enrollment</td>
</tr>
<tr>
<td>Enrollment by Diversity</td>
</tr>
<tr>
<td>White not Hispanic or Latino:</td>
</tr>
<tr>
<td>Hispanic or Latino:</td>
</tr>
<tr>
<td>Asian:</td>
</tr>
<tr>
<td>Black or African American:</td>
</tr>
<tr>
<td>Asian Indian and Alaska Native:</td>
</tr>
<tr>
<td>Native Hawaiian/Other Pacific Islander:</td>
</tr>
<tr>
<td>Other:</td>
</tr>
<tr>
<td>Teachers</td>
</tr>
<tr>
<td>Full-time Teachers:</td>
</tr>
<tr>
<td>Student – Teacher Ratio:</td>
</tr>
<tr>
<td>Percentage of Teachers Certified:</td>
</tr>
<tr>
<td>3 or more years of experience:</td>
</tr>
<tr>
<td>Full-time counselors:</td>
</tr>
<tr>
<td>Test Scores</td>
</tr>
<tr>
<td>Math Proficiency:</td>
</tr>
<tr>
<td>Reading Proficiency:</td>
</tr>
</tbody>
</table>

Table 7: Chandler High School General Demographics (Chandler, 2021)

4.1.c.i Chandler Program Profile Analysis

The entirety of the Chandler High School Program Profile can be found in Appendix K. This section will highlight some of the important data collected for the program at this school.

The program completed its first year during the 2022 – 2023 academic year with 82 students. Student enrollment is depicted by grade in Figure 12. The cybersecurity program will graduate
four students in 2023. Figure 13 depicts the graduates and chosen pathway post-graduation; however, pathway data for 2023 graduates were not available at the time of this study.

**Figure 12: Chandler Cyber Program Student Enrollment**

**Figure 13: Chandler High School Cybersecurity Program Graduates**

Student diversity within the Chandler cybersecurity program is like the overall school demographics with most students identifying as one of the listed minority categories.

Additionally, approximately 22% of students in the cybersecurity program are female. These demographics represent higher diversity than other programs nationally. Demographic specifics
and the comparison between Chandler High School and the cybersecurity program are outlined in Figure 14.

**Figure 14: Chandler High School and Cybersecurity Program Demographics**

The operational aspects of the cybersecurity program consist of personnel, equipment, network, and facilities. The program is primarily supported by one Full Time Equivalent (FTE) teacher. The FTE has transitioned during the academic year due to the primary teacher quitting early in the academic year. The Basha High School program director took over teaching responsibilities until a new FTE was hired in the 3rd Quarter. This is another example of the national shortage of cybersecurity teachers at all academic levels. The itemized initial equipment list for year one operations is in Appendix K. Initial startup costs were approximately $25,600. Additionally, the program required a separate network from the primary school district network. The isolated network was installed in the cybersecurity classrooms and lab spaces to allow access to websites and resources to facilitate learning objectives that would be blocked on the district network. This isolation also required separate hardware due to restrictions on district-provided equipment. Finally, the program has two dedicated learning areas. There is one general-purpose classroom and one CTE lab. The CTE lab has a larger footprint consisting of a teaching space and a space for hands-on activities and equipment storage.
The formal, non-formal, and informal learning activities and pathways are based on the Basha High School cybersecurity program and follows the same curriculum and utilizes the same resources. Since these elements were covered in the Basha High School program profile section, this section will focus on the development methodology for this program. Chandler High School’s cybersecurity program development benefited from the experience and lessons learned of the Basha High School cybersecurity program director and the establishment of the program at Basha High School. The Chandler High School program was modeled on the cybersecurity program at Basha High School. The decision was made to scaffold course offerings as students enrolled and progressed through the program. This decision reduced the teacher requirement which was vital due to personnel turnover.

4.2 Initial Interview Results and Analysis

Interviews were conducted with the cybersecurity program director and individuals involved in program development. Study participants were asked the Interview Questions outlined in the Methodology section to identify the programmatic elements, motivations, challenges, and opportunities identified during program development. This section will outline the results from the interviews conducted for the programs at Basha High School and Chandler High School. As outlined in the program profiles, there are a total of four FTE teachers supporting the programs. One FTE teacher is the program director, two FTE teachers teach within the cybersecurity program at Basha High School in network security and computer science, and one FTE teacher at Chandler High School recently started and is currently completing the CTE certification process to begin teaching during the Fall 2023 semester. Three of the four FTEs were interviewed during this study. The recently hired teacher at Chandler High
School was not interviewed due to a lack of knowledge of the program development and not having taught within either program.

4.2.a Motivation and Program Development

The primary motivation for the cybersecurity program development was based on a school district initiative. An administrator from Chandler School District attended a conference at the University of Arizona (UA) which included stakeholder discussions on developing cybersecurity programs. The district administrator was presented with the pathway from Chandler Gilbert Community College (CGCC) to UA and decided to develop a dual enrollment pathway to CGCC from Basha High School. Basha High School was selected due to the available land and planned development of the building which now houses the Institute of Cyber Operations and Networking (ICON). The program director previously taught cybersecurity courses at another high school and was identified and eventually hired to establish the program at Basha High School. When asked about personal motivation to develop the program, the director stated:

“I attended a lot of conferences while preparing the course in cybersecurity. The cybersecurity community was welcoming, there wasn’t competition among teachers and industry professionals, there was an obvious need for cybersecurity education, and I understood the importance. I took the opportunity to make the biggest difference to the biggest number of students. Cybersecurity offers something for everybody.”

Similarly, the Chandler High School cybersecurity program was developed to make cybersecurity opportunities equitable and services students in the northern area of Chandler in an underserved, underrepresented area. The original intent was to mirror the program at Basha High School; however, there isn’t a clear direction for the future of the program. The Chandler High School program will continue with a staggered implementation until data can be gathered to better provide opportunities aligned with the student population at the school. The program is
exploring alternative certifications such as Cisco Certified Support Technician (CCST) and other certifications to provide post-high school employment opportunities for help desk repair, computer repair, and basic network installation.

Cybersecurity standards, curricular guidelines, and frameworks did not exist when the Basha High School program was developed. The Technical Security Guidelines for Network Security 11.1999.00 CTE requirements were available; however, these were not used initially to develop the program. Despite this, the program must align to these standards which introduces some issues. Computer science, programming, and operating system courses are included in the program which adopts the Arizona Computer Science Standards from the Arizona Department of Education. Additionally, the program includes the ten dual enrollment courses outlined in the program profiles. The CTE and dual enrollment requirements create challenges as described by study participants:

“Meeting CTE requirements is difficult because it is trying to place a square peg in a round hole.”

“Dual enrollment establishes the requirements and standards. These community college courses are sometimes taken by high school freshmen and are rigorous. Since Year 1 students find the courses hard, it can hurt enrollment and we lose students in the program. Other students feel it is great. Seniors realize how far along they are in the discipline.”

“State ADE Computer Science Standards require approval to bring in additional curriculum. Getting resources and approvals for the curriculum is an administrative burden. For example, I put in a request in July 2022 and still waiting on approval in April 2023.”

“Have to follow specific requirements which reduce flexibility and technology changes too fast to follow these timelines.”
4.2.b Operational Elements

The operational elements include instructors, hiring challenges, equipment, networks, and facilities. Recruiting and retaining cybersecurity teachers is challenging. There may be teachers that are ineligible to be CTE-certified or dual enrollment certified in cybersecurity due to a lack of education or experience. Alternatively, you may have industry professionals or people with the appropriate education that do not have teaching experience or are unwilling to teach due to the pay differential. Both cybersecurity programs have had challenges with hiring and retention. The programs have lost teachers for several reasons. One teacher quit within 30 days. This individual was an industry professional with experience teaching post-secondary students but not secondary education. The individual did not feel the opportunity was a fit for them. A qualified teacher from the community college worked at the high school on an interim basis due to a lack of qualified teachers within the cybersecurity program to teach required courses. Another teacher left for industry opportunities with higher salary. Finally, a teacher was relieved of their duties for undisclosed reasons. This demonstrates rapid turnover over the four years of the programs. Compounding this problem is that certifying teachers for CTE or dual enrollment can be lengthy. For example, CTE certification requires classes on teaching, advisory board, and other requirements; state certification, and 140 hours of internship. This process typically takes six months. Alternatively, 5000 hours of industry experience can result in CTE credentialing. Each of these credentialing options represent a significant investment in time impeding the point in time need for teachers in the program. Dual enrollment certification is conducted by the community college and every community college has different certification requirements and processes. Specific comments from study participants included:
“Recruitment and Retention are challenges. Potential teachers don’t fit both molds of CTE and Dual Enrollment. May not be a fit for classroom requirements for secondary education and how to deal with “kids.””

“It was a long process to get dual enrollment certification and to introduce new courses.”

“Money is a barrier. Teaching is a profession that doesn’t yield the same results as industry.”

“Have to have a love for teaching and content expertise. You can write code and automate tasks that can do something repeatedly. Teaching is not like that, and every new year requires a teacher to do things manually over and over again.”

“Professional development and certification can be challenging. Time, funding, and resources can impede getting training.”

The program profiles outline specific equipment, networks, and facilities available to the programs and teachers. All study participants stated that they had the necessary networks and facilities to meet learning objectives and support the program. For equipment, the Technical Standards provided information aligned with the networking aspects but didn’t address cybersecurity holistically. The curriculum and courses dictated equipment requirements. Initial equipment requirements required research on setting up labs, furniture, and space. The school provides basic equipment for classroom instruction; however, the restrictions placed on the machines or their limited technical specifications hinder teaching certain material in the program.

The following are study participant statements regarding networks and equipment:

“District machines do not support cybersecurity education. Had to beg for computers and equipment to support CyberPatriot and other activities. Requested CPU kits for students to build computers associated with A+ / Hardware courses. Everyone has the same equipment for these courses to facilitate teaching and learning.”

“Convincing and justifying the need for equipment not on the pre-approved list was challenging.”

“Had the network but didn’t provide the equipment to utilize the network.”
“Have donated equipment but don’t have the infrastructure to support the equipment. Power to support networking equipment is an example. Would like to set up a cyber or networking range but don’t have the equipment or infrastructure to support it.”

“District has certain restrictions which limit access to certain websites and software that can be loaded on machines. Impedes teaching certain material.”

4.2.c Formal, Non-formal, and Informal Learning Activities

The formal learning activities were built based on the established pathway between CGCC and UA. Individual courses were developed to maintain dual enrollment requirements and the overall pathway. The courses, course description, and syllabi for these courses and their descriptions are outlined in section 4.2 Program Profiles. Additionally, section 4.2 Program Profiles contain the specific non-formal and informal learning activities related to the cybersecurity programs. The discussion of these activities is covered in the program profile section. This section will address the perceived need to include non-formal and informal learning activities into the cybersecurity program. All study participants overwhelmingly agreed that non-formal and informal learning activities are critical to student learning and success. These opportunities provide alternate credentialing in the forms of certifications, experience from internships, and career exploration through externships and guest speakers. Additionally, competitions increase student engagement and understanding of the concepts covered in formal learning activities. Study participants provided the following responses specific to non-formal and informal learning activities:

“Gamification can provide a better perspective for what students learn. Year 1 students learn how to build computers and then students in CyberPatriot make connections to cybersecurity. Provides motivation and interest.”

“Certification is a requirement of CTE. The program must align to a certification. Avenues with each class so that students can seek out opportunities after any year
in the program. Show students the options they have within the curriculum. Stronger more comprehensive foundation.”

“Camps provide the opportunity to work with other kids to develop skills different than course requirements. Builds comradery. Being around like-minded people. Introduces career exploration.”

“Internships and Externships provide paid opportunities in high school. Working directly with the company. Students learned more about the requirements of the workplace. It is exciting and provides opportunities to gain industry experience. “Can’t put a price tag on that experience.””

“Competitions provide a fun learning environment. Drives students to succeed and work as a team. Students are engaged in the process. Competitions make learning great by sharing and reviewing the information from competitions.”

“CTFs, HackTheBox, and CyberPatriot activities keep student interest up. Helps keep students in the program.”

“Introduces kids to alternate learning opportunities or activities to supplement formal learning. Things like Professor Messer can help students with material and lead to certification.”

“Activities like these enhance student engagement and allows them to make sense of where to apply the things they are learning in formal learning activities. The real world application of concepts.”

4.2.d Pathways

The program has the articulated pathway to CGCC and then UA. Although this pathway was a primary driver for program development, the program is designed to provide opportunities for students to enter the workforce, join the military, seek certification training, or attend post-secondary education. The program uses an access database to track students throughout the program. All students are required to complete a program-developed exit survey which asks for personal email addresses and plans post-graduation. Additionally, all students are required to fill out a survey for CTE completion. These surveys are given to students during classroom time to obtain maximum participation. The four-year program provides a solid foundation to pursue
cybersecurity-specific and non-cybersecurity opportunities after graduation. Survey participants provided the following responses regarding pathways:

“The four-year program provides a solid foundation. No matter where they are at in their senior year they have multiple opportunities to choose the pathway. Comprehensive enough to have choices. Cuts down on entry time into the field based on their experience.”

“Hands-down prepares students with applicable information to succeed in fields outside cybersecurity-specific roles. Good employees with a foundation in technology and security. Provides different perspectives since people must interact with people in IT, Finance, and other business functions.”

“Good foundation for other STEM fields such as engineering, biomedical engineering, computer science, and other disciplines.”

“Industry engagement and building in activities into the program builds pathway opportunities for students. Provides tangible things to get students engaged in workforce opportunities.”

“Focus on analysis and problem solving skills that can be applied to other situations.”

“The comprehensive nature of the cybersecurity program can expose students to many different disciplines and if students lose interest in one area they can shift to another while still staying in STEM-related fields.”

Study participant questionnaires and interviews provided the information necessary to develop the program profiles. Additionally, they provided insight into motivation and context bringing additional value to the research study. Upon completion of the interviews, study participants were asked for additional recommendations, identify opportunities, and identify challenges not included in their interview responses. Table 8 provides a breakdown of those responses.
Table 8: Interview Recommendations, Opportunities, and Challenges

<table>
<thead>
<tr>
<th>Recommendations</th>
<th>Opportunities</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Infuse yourself into industry by attending conferences and events to get ideas from others.</td>
<td>• Cybersecurity programs provide pathways to high paying / high opportunity jobs.</td>
<td>• Cybersecurity programs are a new concept for schools and the state. Can be challenging to get buy in for time and resources.</td>
</tr>
<tr>
<td>• Be creative and solve problems.</td>
<td>• The country has a dire need for cybersecurity professionals.</td>
<td>• Need to get administration at the school and district level engaged and bought into the idea.</td>
</tr>
<tr>
<td>• Educate and work with people around you.</td>
<td>• These programs can make students better employees and citizens.</td>
<td>• Should cybersecurity courses be considered “weighted courses”?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CTE requirements to pass certain industry certifications can be challenging.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• School counselor engagement and focus to determine what is best for student instead of forcing them into traditional paradigms. Cybersecurity courses didn’t exist years ago.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Priorities within school: foreign language vs CS courses.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Teachers responsible for marketing their own programs without marketing experience or resources.</td>
</tr>
</tbody>
</table>

4.3 CyberEducation-by-Design Framework

The framework was developed based on the program profiles developed during the case study analysis and integrating disparate elements from the literature review and various elements to make a comprehensive framework.

4.3.a Framework Development

Initial development began by using the foundational elements of Formal, Non-Formal, and Informal Learning defined as:
• Formal Learning – This type of learning is intentional, organized, and structured. Formal Learning opportunities are usually arranged by institutions. Often this type of learning is guided by a curriculum or other type of formal program.

• Non-Formal Learning – This type of learning may or may not be intentional or arranged by an institution, but is usually organized in some way, even if it is loosely organized. There is no form of credit granted in non-formal learning situations.

• Informal Learning – This type of learning is never organized. Rather than being guided by a rigid curriculum, it is often thought of as experiential and spontaneous (Ainsworth, 2010).

Due to the proliferation of opportunities and resources along these three learning models, each can be used separately (Figure 15) or by integrating different aspects in a non-formalized process (Figure 16), or varied combinations along the spectrum of integrating the elements to overcome the underlying problem of a cybersecurity professional shortage.

Figure 15: Separate Learning Paths
These foundational conceptual models are tailored to the study by first breaking down formal education as applied to the U.S. and further delineating those aspects into associated grade and age levels. The pattern of education within the United States consists of Early Childhood Education (ECE), primary or elementary school, middle school, secondary or high school, and post-secondary or tertiary education. Figure 17 depicts the U.S. education levels with grades, ages, and subjects which are integrated into our model (Figure 18). The U.S. Department of Education (DoE) provides the following delineations:

- Post-secondary education includes non-degree programs that lead to certificates and diplomas.
- Post-secondary education includes six degree levels: associate, bachelor, first professional, master, advanced intermediate, and research doctorate.
- Adult and continuing education, plus special education, cut across all education levels (USNEI, 2022).
Figure 17: U. S. Education Levels (USA Hello, 2023)

The formal learning and the fully delineated model becomes the backbone of the proposed framework due to two primary reasons. First, everyone within the U.S. is required to attend school by law. The compulsory school attendance laws vary by state. The complete Table is provided in Appendix C. Arizona students must attend until they are 16 or complete the 10th grade (NCES, 2017). Second, the point of the framework is to inform secondary education institutions and develop cybersecurity knowledge, skills, and abilities to accomplish related tasks.
at a younger age. Finally, integrating informal and non-formal learning opportunities onto the formal education backbone can provide synergy with these goals (Figure 19).

![Diagram of Non-formal Learning Integration](image)

**Figure 19: Non-Formal and Informal Learning Integration**

Like the delineation of formal learning, non-formal and informal learning should be delineated to further refine the model. The activities of these learning models are depicted in Table 9 and described in the following sections. Finally, the aspects of non-formal and informal learning activities are integrated into the framework.

<table>
<thead>
<tr>
<th>Non-Formal Learning Activities</th>
<th>Informal Learning Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camps</td>
<td>Clubs</td>
</tr>
<tr>
<td>Certifications</td>
<td>Competitions</td>
</tr>
<tr>
<td>Internships</td>
<td>Self-Study / Ad-Hoc Learning</td>
</tr>
<tr>
<td>Apprenticeships</td>
<td>Conferences</td>
</tr>
</tbody>
</table>

*Table 9: Non-Formal and Informal Learning Activity Examples*
4.3.b Non-Formal Learning

As previously defined, non-formal learning may or may not be intentional or arranged by an institution, is usually organized in some way, and no formal credits are granted in these learning situations. This section outlines several general examples of non-formal learning opportunities applicable to secondary education.

Camps provide two primary functions that support the framework. The first is to complement or supplement formal education. These camps can be designed to develop general awareness or certain skills through real-world applications and hands-on activities. Second, camps provide outreach activities. Outreach activities have been shown to support student motivation and increase motivation (Wolf, 2020). Additionally, outreach activities can introduce students to STEM-related activities and fields. Despite a focus on STEM, or more specifically cybersecurity, participants in camp and outreach activities result in increased student engagement and overall improvement in educational success (Wolf, 2020).

Certifications matter for three reasons: building confidence; knowledge, skill, and ability, validation; and execution (James, 2018). Additionally, many certifications are typically mapped to learning domains and objectives that can be used to develop cybersecurity curriculum. Further, according to a Burning Glass Technologies report, nearly 60% of cybersecurity positions require at least one certification (Burning Glass, 2019). Thus, certification preparation should be integrated into the framework.

Internships provide real-world experience in work settings and provide career exploration for students. These learning opportunities should provide a supportive environment with learning contexts that are challenging, promote autonomy, present an appropriate degree of structure, and allow for the acquisition of new skills (Gamboa, 2013). Internships for high school students can
validate interests and improve success in pursuing post-secondary education or employment after high school.

Apprenticeships, as identified in the literature review, provide successful transition from student to employee at a high rate. Additionally, apprenticeships provide a vehicle for the students that do not attend post-secondary education which is estimated at 37% of high school completers (NCES, 2020). Apprenticeships can be aligned with curriculum to provide synergy between learning and application.

4.3.c Informal Learning

The case studies identified various non-formal learning opportunities. Informal learning is never organized and is considered experiential and spontaneous. This section outlines several general examples of informal learning opportunities applicable to secondary education.

Clubs are part of the non-formal in-school activities. Participation in clubs have shown that students have higher self-confidence, can persist in competitive situations, and increase choice of and success in STEM related post-secondary majors (Gottfried, 2013). Additionally, clubs provide an environment to develop and pursue creative endeavors (Ahn, 2022).

Competitions can increase interest in the cybersecurity discipline. They provide simulated, real-world scenarios to practice cybersecurity skills across a variety of cybersecurity sub-disciplines. Additionally, competitions encourage teamwork and students can develop in-depth technical knowledge during preparation and execution of the competition (Oliver, 2018). However, competitions are typically seen as extra-curricular activities. Students who participate in competitions in schools that don’t have cybersecurity or related programs tend to lose the obtained knowledge and interest in the subject (Cheung, 2012).
Self-study or ad-hoc learning activities and resources are prolific. These can include online courses, YouTube videos, materials developed by security professionals, podcasts, blogs, and many other resources. These are available at no-cost, low-cost, or through subscription services. Cataloging and aligning these options are outside the scope of this study due to the vast number of materials available. This is added as a category within informal learning as an element of the framework.

Conferences and Industry events provide additional opportunities to learn more about the cybersecurity discipline. Many cybersecurity related events provide workshops, capture the flag events, and other activities to promote cybersecurity awareness and skill development. These events also provide opportunities to connect with industry professionals. Further, participants can attend presentations on recent research and observations in the field.

The integration of these non-formal and informal learning activities aligned to formal learning results in the revised framework model in Figure 20.

![Figure 20: Non-Formal and Informal Learning Activity Examples](image-url)
4.3.d Standards and Guidelines

Standards are essential components in education. They set clear and measurable goals, inform instruction, and assist in the measurement of achievement. Standards can be subcategorized as:

- General Standards – define the knowledge and skills students should possess at critical points in their educational career and serve as the basis of educational reform and measures student success.
- State Standards – standards established at the state level to identify the learning standards defined by grade level which are used to develop curriculum and assessment systems. This is typically done around core subject areas.
- Teaching Standards – used to evaluate educators and determine whether a teacher possesses the attributes of accomplished teaching based on their standards in each certificate area (Education Standards, 2023).

Curriculum guidelines are a document or set of documents that provide guidance for teachers on the following:

- Procedures for successful planning and implementation of curriculum at the school, local, or national level.
- Can focus on a specific learning area or subject, educational level, specific group of learners, or on curriculum.
- Provides ideas, or suggestions and recommendations to help teachers make informed decisions, or be more prescriptive and detailed specifying the content, activities, tasks, and materials to be used by teachers (IBE, 2023).
Several states have developed cybersecurity standards; however, they are primarily tied to computer science and computing programs, related fields, or are lacking. A few examples will be discussed. The Arkansas Computer Science and Computing Standards for High School Cybersecurity are designed to, “provide understandings of concepts in computer science that are necessary for students to function in an ever-changing technological world.” (Addison et al, 2020). The standards follow strands of computational thinking and problem solving; data, information, and security; algorithms and programs; computers and communications; and professionalism and impacts of computing (Addison et al, 2020). Similarly, North Dakota developed the Computer Science and Cybersecurity Standards in 2019 which included cybersecurity standards into the overall document to, “develop citizens of North Dakota that are prepared to live in an increasingly digital and technology-driven society.” (Marsh et al, 2019). Cybersecurity concepts are introduced as part of digital citizenship in grades K-5 and in other areas in later years. Finally, the Arizona Computer Science (CS) Standards’ “Networks and the Internet” essential concepts address cybersecurity (ADOE, 2018). The CS Implementation Guidance identifies the National Integrated Cyber Education Research Center (NICERC) to provide professional development and support for K-12 cybersecurity programs and educators (Mak, 2022). NICERC was rebranded as Cyber.org in 2020. The Network Security 11.1999.00 Technical Standards are a corollary document to Network Security as part of Career and Technical Education (CTE) standards (Network Security, 2019).

For the purposes of this study, the K-12 Cybersecurity Learning Standards from Cyber.org and the High School Cybersecurity Curriculum Guidelines and Glossary from TeachCyber will be used for the framework. The elements from the K-12 Cybersecurity Learning Standards focusing on 9th – 12th grade are provided in Appendix D. Additionally, The
High School Cybersecurity Curriculum Guidelines and Glossary’s Big Ideas, Enduring Understanding, and Learning Objectives are provided in Appendix E. Figures 21, 22, and 23 depict the alignment or crosswalk of Cyber.org’s Learning Standards concepts to TeachCyber’s Learning Objectives across the three core themes of Computing Systems, Digital Citizenship, and Security. This compilation can support teachers in developing, delivering, and assessing cybersecurity concepts at their institutions. It is important to note that the standards and learning objectives could be further delineated; however, that work is outside the scope of this study.

<table>
<thead>
<tr>
<th>Concepts</th>
<th>Standards</th>
<th>Cyber.org Learning Standards For Computing Systems (CS)</th>
<th>TeachCyber Learning Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Communication (COMM)</td>
<td>OSI Model</td>
<td>C2.1.1: Principle of Simplicity</td>
<td></td>
</tr>
<tr>
<td>Network Components (COMP)</td>
<td>Network Diagram</td>
<td>C2.2.2: Principle of Abstraction</td>
<td></td>
</tr>
<tr>
<td>Cloud Computing (CC)</td>
<td>Cloud Computing Risks and Benefits</td>
<td>C2.2.3: Principle of Minimization</td>
<td></td>
</tr>
<tr>
<td>Protocols (PROT)</td>
<td>Ports and Protocols / Risks Online Services</td>
<td>C2.3.7: Principle of Modularity</td>
<td></td>
</tr>
<tr>
<td>Date Less (LOSS)</td>
<td>Risk Mitigation / Redundancy</td>
<td>3.4.1: System Design and Security</td>
<td></td>
</tr>
<tr>
<td>Hardware</td>
<td>Hardware</td>
<td>3.1.1: Communication Layers</td>
<td></td>
</tr>
<tr>
<td>Network Hardware Components (HARD)</td>
<td></td>
<td>3.1.2: Network Standards and Protocols</td>
<td></td>
</tr>
<tr>
<td>Internet of Things (IOT)</td>
<td></td>
<td>2.2.1: Connectivity and Attack Surface</td>
<td></td>
</tr>
<tr>
<td>Operating System (OS)</td>
<td></td>
<td>5.1.1: Hardware and Software Interactions</td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td></td>
<td>5.2.1: Computer Hardware and Related Devices</td>
<td></td>
</tr>
<tr>
<td>Software Updates (SOFT)</td>
<td></td>
<td>5.2.2: Hardware-related Vulnerabilities</td>
<td></td>
</tr>
<tr>
<td>Programming and Scripting (PROG)</td>
<td></td>
<td>5.2.3: Secure Software Development</td>
<td></td>
</tr>
<tr>
<td>Applications (APPS)</td>
<td></td>
<td>5.2.4: Hardware Security Issues – Physical Access</td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td></td>
<td>5.3.1: Software Vulnerabilities</td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td></td>
<td>5.3.2: Secure Software Development</td>
<td></td>
</tr>
<tr>
<td>Hardware</td>
<td></td>
<td>5.3.3: Secure Software Validation</td>
<td></td>
</tr>
<tr>
<td>Network Hardware Components (HARD)</td>
<td></td>
<td>5.4.1: Software and Hardware Vulnerabilities</td>
<td></td>
</tr>
<tr>
<td>Internet of Things (IOT)</td>
<td></td>
<td>5.4.2: Physical System Vulnerabilities</td>
<td></td>
</tr>
<tr>
<td>Operating System (OS)</td>
<td></td>
<td>6.1.3: System Component Impact on Cybersecurity</td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td></td>
<td>7.2.3: Software / Hardware Malicious and Adversary Goals</td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td></td>
<td>7.2.4: Network System Decentralization and Dynamic Nature</td>
<td></td>
</tr>
</tbody>
</table>

*Figure 21: Computing Systems Concepts, Standards, and Learning Objectives Crosswalk*
RING (Regions Investing in the Next Generation) is a National Security Agency (NSA) Center of Academic Excellence in Cybersecurity (CAE-C) K-12 Pathway funded project that involved two coalitions. The University of Alabama Huntsville coalition consisted of Coastline...
Community College, Dakota State University, Pace University, Purdue University Northwest, and Dark Enterprises (Hairston, 2022). The Moraine Valley Community College coalition consisted of Forsyth Technical Community College, Brookdale Community College, Florida State College at Jacksonville, Cal Poly Pomona, and Eastern New Mexico University Ruidoso (Hairston, 2022). RING is “an online high school cybersecurity course that offers interesting and engaging content specifically for students and schools without an existing cybersecurity program” that officially launched in the summer of 2022 (Hairston, 2022). The program is divided into ten units consisting of an introduction, ethics, establishing trust, ubiquitous connectivity, data security, introduction to Python programming, system security, adversarial thinking, risk, and implications. These units align with the TeachCyber Cybersecurity Curriculum Guidelines providing seamless linkage from the “Big Ideas” to the learning objectives of the curriculum. Supporting this curriculum are lesson plans, slides, graphic organizers for vocabulary and concepts, viewing guides, activities, Quizlet, Kahoot, labs, and projects. The general RING contents are outlined in the table in Appendix F, definitions of the curriculum and resources are provided in the glossary, and examples of these items are provided in Appendix G.

Cyber.org provides four cybersecurity-specific courses for K-12 education: Cyber Literacy (Grades 8 – 10), Cyber Literacy II (Grades 9 – 12), Cybersecurity Basics (Grades K – 8), and Cybersecurity (Grades 10 – 12). The basic outline for these courses is:

- Cyber Literacy – hands-on curriculum that introduces students to cyber by blending robotics, programming, electricity, and elements of liberal arts (Cyber Literacy, 2019).
- Cyber Literacy II – project-driven curriculum that expands a student’s understanding of cyberspace through systems engineering and liberal arts (Cyber Literacy II, 2019).
• Cybersecurity Basics – introductory course that is currently under development that will cover the domains of security and digital citizenship (Cybersecurity Basics, 2022).

• Cybersecurity – comprehensive year-long course geared toward educators teaching high school cybersecurity that contains cybersecurity concepts and skills and technical know-how through CompTIA Security+ certification (Cybersecurity, 2022).

For the purposes of this study, the cybersecurity course will be explored in depth as a complimentary program to RING. Cyber.org’s Cybersecurity course contains over 150 activities designed for use in the Cyber.org range at no cost to all U.S. K-12 Educators (Cybersecurity, 2022). Each lesson includes support and supplemental materials which include teaching guides, teacher notes, PowerPoints, guided notes, labs, quizzes, and answer keys for all assessments. The table in Appendix H provides the elements of the cybersecurity curriculum and curriculum examples of these materials are provided in Appendix I. The curriculum is supported by the cyber.org range which provides a secure online environment to allow completion of learning activities and develop skills.

4.3.f Pathways

The U.S. Department of Education’s mission is to, “Promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access” (ED, 2023). This preparation provides a pathway to the next stage of student success. The primary options for high school students upon completion of their secondary education are going straight into the workforce, joining the military, enrolling in a trade or certification program, or enroll into a post-secondary educational institution. Therefore, in addition to developing the requisite knowledge, skills, and abilities to complete their secondary education, the framework should provide the requisite KSAs specific to cybersecurity to ensure students are
able to successfully and/or seamlessly transition into one of the primary post-secondary options (Figure 24).

![Diagram of Post-Secondary Pathway Options]

**Figure 24: Post-Secondary Pathway Options**

Pathway development and articulation agreements are outside the scope of this study. The proposed framework will integrate the general pathway options; however, the details of developing those are outside the scope of this study. Despite this, three important concepts are added due to their potential impact on secondary education institutions and the framework.

Dual enrollment, reverse articulation, and concurrent enrollment are all similar in that they allow a high school student to receive post-secondary credits while still enrolled in high school. The exact definition of these terms and their application vary among institutions and states. Dual Enrollment is a term referring to a student that is enrolled in two distinct academic programs or institutions. For the purposes of this study and in relation to Arizona, dual enrollment is when students receive community college credit for courses that are taken in and at high school. Similarly, concurrent enrollment exists when, “a student is simultaneously enrolled in any combination involving more than one registration or grade level within a school, more
than one school within a district or charter holder, or more than one school in different Arizona public educational agencies (Horne, 2007).” Reverse articulation or reverse credit is the process of receiving credit for courses taken at a subsequent level of education at the preceding level of education. For example, credits completed toward a 4-year degree may be applicable for an associate-level degree. Alternatively, credits obtained at post-secondary institutions may be used toward secondary education requirements.

Additionally, there are several organizations and options to obtain college credit prior to enrolling in post-secondary institutions including Advanced Placement (AP) and College Level Examination Program (CLEP). AP are classes designed and administered by College Board to support students that plan on attending post-secondary education. Research has demonstrated that students that take AP courses are better prepared for college due to their familiarity with college-level work; develop college skills like time management, critical thinking, and scholarly writing; identify student interests and passions; and potentially boost the student Grade Point Average (GPA) (What is AP, 2023). The College Level Examination Program (CLEP) offers 34 exams associated with introductory-level college course material. CLEP provides students several benefits including saving money, saving time, and performing better in college.

The combination of the elements of formal, non-formal, and informal learning; standards and guidelines; curriculum; and pathways can be viewed comprehensively in Figure 25. The relationships among these elements and the supporting content develop qualified and competent cybersecurity professionals to overcome the cybersecurity workforce gap with a focus on secondary education.
Figure 25: Comprehensive CyberEducation-by-Design Framework

4.4 Framework Interview Results and Analysis

The framework interview questions were designed to provide initial validation and recommendations. The framework was presented to study participants to gather initial insight into the framework and its elements. Framework interview questions are outlined in the Methodology section.

The framework identified and defined different elements of formal, non-formal, and informal learning activities inclusive of the elements identified by the case study for the programs at Basha and Chandler High Schools and activities in general. The inclusion of standards, guidelines, and curriculum examples was seen as beneficial to provide guidance to teachers and to articulate needs to administrators. Two specific responses include:

“Standards, guidelines, and curriculum help shape the program and are what teachers seek. Teachers want to know what the guidelines and state requirements are.”

“Standards and guidelines would have helped focus interactions with administrators to further initiatives and overcome objections.”
The interviews identified several ways in which the proposed framework would have assisted in the development of the cybersecurity education program at these institutions. The generalized nature of the framework with the specific examples of the program profiles, equipment lists, and curriculum outlines and examples provide a starting point for new programs. The inclusion of Cyber.org and the RING curriculum provides flexibility to introduce fully developed cybersecurity courses and scale to a program when resources, faculty, and support exist. Study participants provided the following comments related to this:

“The framework provides a starting point to develop the program, understand startup costs associated with equipment and software, and other resources to make informed decisions on how to establish the program.”

“The information provided in the framework can help articulate programmatic needs and alignment with national standards.”

Resource examples provide information about informal learning to supplement formal learning objectives. Study participants identified the lack of a central repository for resources at the K-12 level or access to opportunities. Additionally, there is a lack of engaging content in some subject areas created for this age group. Specific responses from study participants include:

“Higher education or groups need to develop more engaging, age appropriate ways to teach dry content.”

“The only way I knew about the Melissa Dark opportunity was because I joined a Facebook group for cybersecurity educators.”

Based on the interview results, it was recommended to include additional information applicable to the Arizona Department of Education’s CTE requirements aligned with the Network Security requirements. The Network Security 11.1999.00 Program Description, Industry Credential, Cohort Sequence, and Teacher Certification Document, Blueprint for Instruction and Assessment, and Instruction Framework were added to Appendix N, Appendix O, and Appendix P respectively. Although the identification of these missing elements was
identified, it is important to note that these requirements and guidance are state-specific, CTE-specific, and network security specific. The applicability of these standards to cybersecurity was identified by all study participants as lacking the requirements necessary to develop a comprehensive cybersecurity program. Additionally, it was recommended that the Cyber.org range be listed under informal learning opportunities.

“I introduce the cyber range to Year 1 networking students to integrate security concepts into the course. There is little discussion of security concepts due to course alignment with the Technical Standards. It also generates interest in students.”

Cyber.org is included in the curriculum portion of the framework since the curriculum is aligned with activities that are integrated into the range. Listing it within the program profiles makes sense to demonstrate multiple uses for these free and open-source resources providing an avenue for institutions to introduce cybersecurity concepts without the overhead of a full course or program.
CHAPTER 5

Conclusions

5.1 Summary of the Research

This study outlined the overarching problem of a shortage of cybersecurity professionals to meet the workforce needs globally. The growth in sophistication, scope, and scale of cybersecurity threats exacerbates this problem. Stakeholders from K-12 education, post-secondary education, employers, and aspiring cybersecurity professional each have a role in overcoming this problem.

The literature review first reviewed government legislation that identified national needs for cybersecurity education and government support for these needs. Every president since President Bush in 2003 identified a need for cybersecurity education programs to support workforce development and ultimately national security. Initiatives included developing or expanding cybersecurity awareness and training, developing the Cybersecurity Framework, implementing the Cybersecurity National Action Plan, expanding the pool of cybersecurity candidates, identifying the shortage of cybersecurity teachers at all educational levels, and development of the K-12 Cybersecurity Act are a few examples of these initiatives.

The literature review then identified and evaluated standards organizations and their applicability to the identified problem. National Institute of Science and Technology’s (NIST) SP 800-181: Workforce Framework for Cybersecurity, National Security Agency’s NCAE-C program, the Joint Task Force on Cybersecurity Education’s Cybersecurity Curriculum Guidelines and the Association for Computing Machinery’s (ACM) Cybersecurity Curricular Guidance for Associate-Degree programs, TeachCyber’s High School Cybersecurity Curriculum
Guidelines, and Cyber.org’s K-12 Cybersecurity Standards were evaluated to identify the current state of the standards and guidelines applicable to this space.

The literature then focused on curricula and current initiatives available to support cybersecurity education. There are currently hundreds of hours of content provided by organizations like the National Cybersecurity Training and Education (NCyTE) Center, Cyber.org, Centers of Academic Excellence in Cybersecurity Resource Directory (CARD), Cybersecurity Labs and Resource Knowledge Base (CLARK), and Regions Investing in the Next Generation (RING) program. The current solutions focused on cyber-safety, cyber-education, and cyber-skills which included information on certifications, internships, apprenticeships, on-the-job training, and experiential learning.

This background identified the gaps to develop the research problem, purpose of the study, and objectives. The purpose of the study was to create comprehensive program profiles of existing cybersecurity education programs at secondary education institutions in Arizona. These profiles were developed through open-source research and interviews with key personnel that developed the programs within the scope of the study. The obtained data were used to develop a general CyberEducation-by-Design framework with the goal of providing a starting point document for the future development of cybersecurity education programs at secondary education institutions. Finally, key personnel interviewed during program profile development were presented with the framework to gather initial input on the validity, viability, and comprehensiveness of the framework. Specifically, these second interviews were used to determine whether the framework contained the necessary elements and activities related to formal, non-formal, and informal learning activities; inclusion of standards, guidelines, and
curriculum; how the framework would have supported initial program development; and identify any gaps, limitations, or recommendation to improve the framework.

This study was successful and exceeded the original objectives set forth at the beginning of the study. The interviews provided insights into the development of cybersecurity programs at secondary education institutions. These interviews assisted in developing the program profiles which further informed the development of the CyberEducation-by-Design framework. Secondary interviews provided feedback on the framework’s design. This allowed for an initial iteration and improvement cycle. Where the study exceeds the objectives were the identification of lessons learned, best practices, challenges, and opportunities. These elements may not be applicable to all schools; however, they may save time and resources when establishing new cybersecurity programs at secondary education institutions.

5.2 Highlights and Key Contributions

This study provided multiple insights which resulted in two primary outcomes that will have implications within the state and potentially the nation. The developed program profiles provide a structure to analyze other programs internal or external to Arizona. The enhanced data set can provide the ability to compare programs to develop best practices for establishing cybersecurity education programs at secondary education institutions. These profiles can allow schools considering the development of a program at their institutions to better understand the requirements and resources needed to establish the program. Additionally, the data collected can provide a baseline to compare their district and school to understand the implications within the context of their environment. Finally, the profiles identify existing opportunities for non-formal and informal cybersecurity learning activities to expose students to cybersecurity KSAs without
building an entire program. This has implications for the field and supports student development within Science, Technology, Engineering, and Math (STEM).

Another outcome was the development of the CyberEducation-by-Design framework. The framework identifies the formal, non-formal, and informal learning activities that can be integrated into a comprehensive program. These elements provide the ability to develop the necessary competencies to meet the cybersecurity work roles defined by NIST. The framework identifies generic examples of these learning activities while the program profiles provide specific examples. Additionally, the framework crosswalks the Cyber.org standards with the TeachCyber curricular guidelines. Further, the framework aligns these standards with the RING and Cyber.org curricula. Finally, pathways are introduced to identify subsequent opportunities for students.

5.3 Limitations

The scope of this study was to analyze cybersecurity education programs at secondary education institutions within Chandler, AZ. The literature review identified that cybersecurity standards and curriculum guidelines for secondary education institutions were not available until 2021. Additionally, most state standards do not specifically address cybersecurity education. Cybersecurity, if included at all, is included within computer science, information technology, or other CTE program areas. This lack of foundational guidance means that existing programs across districts and states may not align with the required KSAs to meet industry needs. At the time the study was conducted, Arizona only had two comprehensive cybersecurity programs being offered. The fact that the programs were within the same school district further limited the diversity of data collected. Finally, time was factored in to properly scope the study. Conducting interviews with study participants, developing program profiles on two cybersecurity programs,
developing the initial CyberEducation-by-Design Framework, reinterviewing study participants to gather feedback on the framework, and updating the framework was accomplished during this study. Given more time, additional feedback sessions with other stakeholders could have been conducted to further refine the framework.

5.4 Future Work

The goal of research and the dissertation is to advance the science and subject matter. More importantly, these activities can identify future work that can be conducted on the specific topic or branch off into corollary research. The scope of this research study was appropriate; however, it identified several opportunities for future research.

5.4.a Further Framework Validation and Program Profile Development

The case study included cybersecurity programs at two institutions within Arizona. This provided insight along with additional research and analysis to create the initial CyberEducation-by-Design Framework. Additionally, interviews were conducted to provide initial feedback from case study participants on the framework value and assess its elements. This feedback provided the opportunity to refine the framework. This work provides two opportunities for additional research within this area. First additional program profiles could be developed at institutions across the country to develop a broader range of profiles. Second, interviews and focus groups could be conducted with different stakeholders to evaluate and provide input into the framework to further refine the document. This could be done within Arizona with schools interested in starting a cybersecurity education program. Additionally, the scope of stakeholders could be expanded to include administrators, teachers, and staff that are either involved in cybersecurity education or have interest in supporting these programs. Finally, the framework could be expanded to other states or nationally.
5.4.b Expanding Framework

The study and current framework focused on secondary education programs. Similarly, the TeachCyber Curriculum Guidelines focus on secondary education. Considering Cyber.org’s Cybersecurity Learning Standards are comprised of grades K-12, the framework could be expanded to include Early Childhood Education (ECE), Elementary, and Middle School. The ability to integrate cybersecurity concepts at a younger age benefits the individual, families, and society in general by making them cyber literate and more cyber secure. Alternatively, the other end of the framework could be further expanded to further identify and develop pathways to inform the elements of the framework at different grade levels.

5.4.c Teacher Development and Hiring

Cybersecurity educators are lacking at all educational levels. Cybersecurity programs and program development is not sustainable without the teachers to support the programs. The ability to identify and hire qualified cybersecurity teachers for secondary education is challenging. Certifying or credentialing current teachers to teach cybersecurity is an option; however, can be challenging due to differing credentialing requirements which vary among districts and states and the required time to meet the requirements can be extensive. Research could be conducted to identify ways to locally support training and credentialing, or national initiatives could be developed. For example, the National Cybersecurity Teaching Academy provides 18-credit hour graduate certificates for high school teachers to meet credentialing requirements (NCTA, 2023).

5.4.d State Standards

State standards focusing on cybersecurity could be catalogued, compared, and analyzed to develop best practices or a template to support the development of cybersecurity state standards. State standards were reviewed to identify how cybersecurity requirements were
integrated to support framework design. If cybersecurity is addressed at all, they are often integrated into network security or other CTE requirements or fall under computer science related standards. Developing state standards for cybersecurity can help promote cybersecurity and require the concepts to be integrated into formal education.

5.4.e Longitudinal Studies

Finally, this work and the expansion of cybersecurity education into middle and high schools lends itself to longitudinal studies. These longitudinal studies could focus on current students and track their ability to meet specific requirements for certain job roles during the four-year program. Another option would be to track students after graduation and collect data through the lens of pathways. Determining whether the program adequately prepared students for post-secondary education, military service, certification and trade programs, or directly into the workforce could identify opportunities for program improvement and understand workforce development aspects.
REFERENCES


https://dese.ade.arkansas.gov/admin/Files/20210205094013_CSforAR_High_School_Cy bersecurity_12152020_PDF.pdf.


https://www.caecommunity.org/cae-map.


Northwestern University.


https://www.ccslearningacademy.com/cybersecurity-bootcamps-everything-you-need-to-know-including-the-competitive-salary-ranges/#:~:text=No%20course%20on%20earth%20can,cybersecurity%20after%20completing%20the%20course.


https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf.

CCSEC (2020, February 1). Cybersecurity Curricular Guidance for Associate-Degree Programs. ACM Committee for Computing Education in Community Colleges.


https://www.census.gov/quickfacts/chandlercityarizona.


https://www.nabyte.net/resources/cybersecurity-curriculum.


https://www.caeresource.directory/home.


https://clark.center/home.


https://www2.ed.gov/about/landing.jhtml.


https://educationdata.org/number-of-college-graduates#:~:text=The%20total%20number%20of%20graduates,graduated%20in%202020.


Arizona Department of Education.


Kharbach, M. (2022, October 12). What is Quizlet and How to Use it to Create Interactive Flashcards and Quizzes? Educational Technology and Mobile Learning.


Maricopa County (2022). Maricopa County, AZ. Data USA.  
https://datausa.io/profile/geo/maricopa-county-az#housing

https://doi.org/10.48009/3_iis_2018_193-201.


https://scholar.dsu.edu/cgi/viewcontent.cgi?article=1365&context=theses.


https://caecommunity.org/initiative/k12-ring#:~:text=What%20is%20RING%3F,without%20an%20existing%20cybersecurity%20program.


USA Hello (2023). What are the U.S. education levels? USA Hello.
https://usahello.org/education/children/grade-levels/

https://www2.ed.gov/about/offices/list/ous/international/usnei/edlite-index.html.


Assessment Method – measures whether students learned a lesson’s information and met your lesson objectives. Options include quizzes, hands-on activities, writing assignments, group presentations, or class journal entries (Stauffer, 2019).

Case Studies (Cyber.org) – involves a scenario that happened in the real world, each of which contains an entire article, a teacher summary, guided questions, and links for further readings. Students engage via guided questions provided by teachers to the students (Cybersecurity, 2022).

Concurrent Enrollment – situation where a student is enrolled in two distinct academic institutions at the same time.

Cyber Range (Cyber.org) – virtual lab environment where students can simulate cybersecurity scenarios in a safe, protected online environment as they explore the back end of IT systems (Cybersecurity, 2022).

Dual Enrollment – a term referring to a student that is enrolled in two distinct academic programs or institutions. Specifically, community college courses that are taken at and in high school.

Formal Learning – This type of learning is intentional, organized, and structured. Formal Learning opportunities are usually arranged by institutions. Often this type of learning is guided by a curriculum or other type of formal program (Ainsworth, 2010).

Graphic Organizers – a visual and graphic display that depicts the relationships between facts, terms, and/or ideas within a learning task. Graphic organizers are sometimes referred to as knowledge maps, concept maps, story maps, cognitive organizers, advance organizers, or concept diagrams (Graphic Organizers, 2023).

Informal Learning – This type of learning is never organized. Rather than being guided by a rigid curriculum, it is often thought of as experiential and spontaneous (Ainsworth, 2010).

Kahoot – a cloud-based quiz platform and digital learning platform that uses quiz-style games to help students learn (Edwards, 2022).

Lesson Materials – List of materials that needed to teach the lesson and measure student outcomes. These include student handouts, textbooks, visual aids, grading rubrics, activity packets, and computers/tablets (Stauffer, 2019).

Lesson Objectives – list what students will be able to do after completing the lesson. Objectives should be Specific, Measurable, Attainable, Relevant, and Time-Based (SMART) (Stauffer, 2019).
Lesson Plans – a teacher’s daily guide for what students need to learn, how it will be taught, and how learning will be measured. Lessons plans have six key parts: lesson objectives, related requirements, lesson materials, lesson procedures, assessment method, and lesson reflection (Stauffer, 2019).

Lesson Procedure – in-depth explanation of how the lesson will progress in the classroom. These are done in four phases: explore (1): students discover a concept, learn and practice (2): students apply their discoveries, reflect (3): students review what they have learned, and reinforce (4): students apply their knowledge to problem solving scenarios (Stauffer, 2019).

Lesson Reflection – Portion of a lesson plan that encourages teachers to take notes on how to improve a lesson after it has been completed (Stauffer, 2019).

Quizlet – a web tool and a mobile application that provides study tools such as flashcards and game-based quizzes (Kharbach, 2022).

Quizzes (Cyber.org) – assessments associated with the 155 lessons in either multiple choice, multiple selection, or true / false format provided in Word or Question and Test Interoperability (QTI) format (Cybersecurity, 2022).

Related Requirements – national, state, or school standards that dictate what you need to teach in a class (Stauffer, 2019).

Reverse Articulation / Credit / Transfer – the process of receiving credit for courses taken at a subsequent level of education at the preceding level of education.

Viewing Guides – a type of lesson material used by the RING framework to guide student learning after watching video based learning material.

Labs – or laboratory activities enable learners / students to obtain a range of practical skills through experiments and experience allowing them to have a better understanding of the content (Hurix, 2022).

Labs (Cyber.org) – hands-on lab exercises in the form of attack, example, or tool that help support the lessons.

- Attack Lab – show the students a real-world example of how a malicious user can attack an unsuspecting user’s system and how this user can defend themselves.
- Example Lab – has students run through a concept and see an example of how things work.
- Tool Lab – has students explore different tools used in pen and vulnerability testing (Cybersecurity, 2022).

Lessons (Cyber.org) – align to CompTIA Security + objectives broken down into 155 individual lesson which contains a PowerPoint to guide the teacher in delivering the material to students (Cybersecurity, 2022).
Non-Formal Learning – This type of learning may or may not be intentional or arranged by an institution, but is usually organized in some way, even if it is loosely organized. There are no form of credits granted in non-formal learning situations (Ainsworth, 2010).

Projects – or project based learning is a teaching method in which students learn by actively engaging in real-world and personally meaningful projects (PBL, 2023).

QTI (Question and Test Interoperability) – the de-facto standard for e-assessment interoperability. Identifies and defines the formats, protocols, and points of interoperability that save users and suppliers time and money in development, delivery, and outcomes of assessments (1Edtech, 2023).

Teacher Notes (Cyber.org) – intended to be used to provide background and explain the different concepts for the teacher who will be guiding the class (Cybersecurity, 2022).
APPENDICES

Appendix A: SLR TABLE

<table>
<thead>
<tr>
<th>Authors</th>
<th>Year</th>
<th>Title</th>
<th>Category</th>
<th>Main Findings</th>
</tr>
</thead>
</table>
| Bush, G.   | 2003 | The National Strategy to Security Cyberspace                          | Government Legislation        | • Promote a comprehensive national awareness program to empower all Americans; businesses, the general workforce, and the general population, to secure their own parts of cyberspace.  
• Foster adequate training and education programs to support the Nation’s cybersecurity needs.  
• Increase the efficiency of existing general cybersecurity training programs.  
• Promote private-sector support for well-coordinated, widely recognized professional cybersecurity certifications |
| CISA       | 2020 | Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure | Government Legislation      | • The U. S. cybersecurity workforce needs immediate and sustained improvements.  
• It is necessary to expand the pool of cybersecurity candidates through retraining and by increasing the participation of women, minorities, and veterans.  
• There is a shortage of cybersecurity teachers at the primary and secondary levels, faculty in higher education, and training instructors.  
• Comprehensive and reliable data about cybersecurity workforce positions needs and education and training programs are lacking |
• Conduct an evaluation of the challenges K-12 educational institutions face in securing information systems and student records and implementing cybersecurity protocols.  
• Identifying challenges related to remote learning. |
<table>
<thead>
<tr>
<th>Authors</th>
<th>Year</th>
<th>Document Title</th>
<th>Standards Organizations</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Breaks down 33 specialized areas with these categories.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Aligns the Knowledge, Skills, and Abilities to complete defined tasks</td>
</tr>
<tr>
<td>CSEC</td>
<td>2017</td>
<td>Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity</td>
<td>Standards Organizations</td>
<td>• Outlines eight knowledge areas.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Identifies cross cutting concepts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Identifies knowledge area essentials and provides knowledge units and topics within the knowledge areas</td>
</tr>
<tr>
<td>CCECC</td>
<td>2020</td>
<td>Cybersecurity Curricular Guidance for Associate-Degree Programs</td>
<td>Standards Organizations</td>
<td>• Guidelines for:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• conducting programs review to update and create curriculum.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• facilitating program and course articulation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• complying with government-sponsored frameworks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• interacting with local advisory boards</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Provides a means or organizing and managing content in a systematic way.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Enables educators to effectively plan properly sequenced activities to provide learning opportunities targeting desired learning outcomes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Ensure students develop a base of knowledge, skills, attitudes, beliefs, and values to function successfully in cybersecurity college programs and careers</td>
</tr>
<tr>
<td><strong>Cyber.org</strong></td>
<td>2021</td>
<td>K12 Cybersecurity Learning Standards</td>
<td>Standards Organizations / Curriculum</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>------</td>
<td>-------------------------------------</td>
<td>--------------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Outlines core cybersecurity themes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Breaks down core themes into sub concepts, topics, and standards by grade band</td>
<td></td>
</tr>
<tr>
<td><strong>S. Edwards</strong></td>
<td>2021</td>
<td>Cyber-Safety and COVID-19 in the early years: A research agenda</td>
<td>Cyber-Safety</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Internet use amongst young children increased during COVID-19</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Cyber-safety education in early years is under-research and insufficiently provided for in practice.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Critical constructivism which is concerned with the relationship between people, technologies, and societies to guide research in young children</td>
<td></td>
</tr>
<tr>
<td><strong>N. Arfi and S. Agarwal</strong></td>
<td>2013</td>
<td>Knowledge of Cybercrime among Elderly</td>
<td>Cyber-Safety</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Types of cybercrime against elderly</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Problems of Cybercrime against elderly</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Factors that contribute to increased risk of Elderly</td>
<td></td>
</tr>
<tr>
<td><strong>E. Sobiesk, J. Blair, G. Conti, M. Lanham, and H. Taylor</strong></td>
<td>2015</td>
<td>Cyber Education: A Multi-Level, Multi-Discipline Approach</td>
<td>Cyber-Education</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Cyber Education Project (CEP): Cyber Sciences</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Multi-Level, Multi-Discipline Approach to Cyber Education</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Value of extracurricular enrichment opportunities</td>
<td></td>
</tr>
<tr>
<td><strong>M. McNulty</strong></td>
<td>2021</td>
<td>Cybersecurity Education for Non-Technical Learners</td>
<td>Cyber-Education</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Students in non-technical programs demonstrate a general deficiency in technical knowledge of cybersecurity concepts.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Develop and integrate a cybersecurity general education course for all students.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Develop and integrate cybersecurity content or courses that are complementary to the program of study</td>
<td></td>
</tr>
<tr>
<td><strong>E. Glantz, M. Bartolacci, M. Naseredding, and D. Fusco</strong></td>
<td>2020</td>
<td>Cross-Boundary Cyber Education Design</td>
<td>Cyber-Education</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Cross-boundary process guiding undergraduate cyber education.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Advertise modules that align with certification exams.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Develop courses with input from industry to match industry needs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Develop a wide variety of courses given resource constraints</td>
<td></td>
</tr>
<tr>
<td>Authors</td>
<td>Year</td>
<td>Title</td>
<td>Cyber-Skills</td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>
| J. Marquardson and A. Noshokaty | 2019 | Skills, Certifications, or Degrees: What Companies Demand for Entry-level Cybersecurity Jobs | • Identified avenues for achieving entry-level jobs: skills, certifications, college degree.  
• Analyzed 11,938 entry-level cybersecurity job postings:  
  • 60% require college degree.  
  • 24% prefer college degree.  
  • 29% require a certification. |
| J. James and J. Callen   | 2018 | Cybersecurity Certifications Matter                                  | • Certifications matter: Confidence, Validation, Execution                    |
|                         |      |                                                                      | • Cybersecurity certifications can increase KSAs and give students an edge when applying for jobs.  
• Co-curricular activities such as competitions, journals, webinars, and seminars can enhance KSAs |
| S. Jarocki and H. Kettani| 2019 | Examining the Efficacy of Commercial Cyber Security Certifications for Information Security Analysts | • Value and Effectiveness of cybersecurity certifications  
• Research is limited on efficacy of commercial incident response cybersecurity certifications in selecting potential candidates |
| K. Knapp, C. Maurer, and M. Plachkinová | 2017 | Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance | • Factors impacting the maintenance of cybersecurity certifications.  
• Appropriateness of using certifications for curriculum shaping  
• Experiential Learning and Capstone Courses |
| G. Stoker, U. Clark, M. Vanajakumari, and W. Wetherill | 2021 | Building a Cybersecurity Apprenticeship Program: Early-Stage Success and Some Lessons Learned | • NICE Working Group on Apprenticeships  
• Cyberstart Apprenticeship  
• Cybersecurity Youth Apprenticeship Initiative |
| A. Goín, C. Branter, L. Johnston, R. Rodriguez, and J. Hott | 2021 | Idaho Cyber Heroes: Helping Individuals Navigate Career Pathways in Cybersecurity | • Increasing Career Awareness in High Schoolers  
• Requirements and Barriers for a Career in Cybersecurity  
• Benefits of Internships and Apprenticeships |
| White House  | 2022 | FACT SHEET: Biden-Harris Administration accomplishments Cybersecurity Apprenticeship Sprint | Cyber-Skills | • Lack of Diversity in the Cybersecurity Workforce | • Opportunity presented by internship opportunities. | • Results of 120 day apprenticeship initiative |
# Appendix C: Compulsory School Attendance Laws By State: 2017

<table>
<thead>
<tr>
<th>State</th>
<th>Age of required school attendance</th>
<th>Minimum age limit to which free education must be offered</th>
<th>Maximum age limit to which free education must be offered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alabama</td>
<td>6 to 17</td>
<td>5</td>
<td>17</td>
</tr>
<tr>
<td>Alaska</td>
<td>7 to 16 ¹</td>
<td>5</td>
<td>20</td>
</tr>
<tr>
<td>Arizona</td>
<td>6 to 16 ²</td>
<td>6</td>
<td>21</td>
</tr>
<tr>
<td>Arkansas</td>
<td>5 to 18</td>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td>California ³</td>
<td>6 to 18</td>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td>Colorado</td>
<td>6 to 17</td>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td>Connecticut</td>
<td>5 to 18 ⁴</td>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td>Delaware</td>
<td>5 to 16</td>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td>District of Columbia</td>
<td>6 to 16 ²</td>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td>Florida</td>
<td>6 to 16</td>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td>Georgia</td>
<td>6 to 16</td>
<td>5</td>
<td>19</td>
</tr>
<tr>
<td>Hawaii</td>
<td>5 to 18</td>
<td>5</td>
<td>20</td>
</tr>
<tr>
<td>Idaho</td>
<td>7 to 16</td>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td>Illinois</td>
<td>6 to 17</td>
<td>4</td>
<td>21 ⁵</td>
</tr>
<tr>
<td>Indiana</td>
<td>7 to 18</td>
<td>5</td>
<td>22</td>
</tr>
<tr>
<td>Iowa</td>
<td>6 to 16 ¹⁰</td>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td>Kansas</td>
<td>7 to 18</td>
<td>5</td>
<td>21 ¹¹</td>
</tr>
<tr>
<td>Kentucky</td>
<td>6 to 16</td>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td>Louisiana</td>
<td>7 to 18</td>
<td>5 ¹²</td>
<td>20 ¹³</td>
</tr>
<tr>
<td>Maine</td>
<td>7 to 17</td>
<td>5 ¹⁴</td>
<td>20</td>
</tr>
<tr>
<td>Maryland</td>
<td>6 to 18</td>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td>Massachusetts</td>
<td>6 to 16</td>
<td>3 ¹⁵</td>
<td>22</td>
</tr>
<tr>
<td>Michigan</td>
<td>6 to 18</td>
<td>5</td>
<td>20</td>
</tr>
<tr>
<td>Minnesota</td>
<td>7 to 17</td>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td>Mississippi</td>
<td>6 to 17</td>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td>Missouri</td>
<td>7 to 17 ¹⁶</td>
<td>5 ¹⁷</td>
<td>21</td>
</tr>
<tr>
<td>Montana</td>
<td>7 to 16 ¹⁸</td>
<td>5</td>
<td>19</td>
</tr>
<tr>
<td>Nebraska</td>
<td>6 to 16</td>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td>Nevada</td>
<td>7 to 18</td>
<td>5</td>
<td>21 ¹⁹</td>
</tr>
<tr>
<td>New Hampshire</td>
<td>6 to 18</td>
<td>—</td>
<td>21</td>
</tr>
<tr>
<td>New Jersey</td>
<td>6 to 16</td>
<td>5</td>
<td>20</td>
</tr>
<tr>
<td>New Mexico</td>
<td>5 to 18</td>
<td>5</td>
<td>—</td>
</tr>
<tr>
<td>New York</td>
<td>6 to 18 ²⁰</td>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td>North Carolina</td>
<td>7 to 16</td>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td>North Dakota</td>
<td>7 to 16</td>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td>Ohio</td>
<td>6 to 18</td>
<td>5</td>
<td>22</td>
</tr>
<tr>
<td>Oklahoma</td>
<td>5 to 18</td>
<td>5 ²¹</td>
<td>21</td>
</tr>
<tr>
<td>Oregon</td>
<td>6 to 18</td>
<td>5</td>
<td>19 ²²</td>
</tr>
<tr>
<td>Pennsylvania</td>
<td>8 to 17</td>
<td>6 ²³</td>
<td>21 ²⁴</td>
</tr>
<tr>
<td>Rhode Island</td>
<td>6 to 18 ²⁵</td>
<td>5</td>
<td>21 ²⁶</td>
</tr>
<tr>
<td>South Carolina</td>
<td>5 to 17</td>
<td>5</td>
<td>22 ²⁷</td>
</tr>
<tr>
<td>South Dakota</td>
<td>6 to 18 ²⁸</td>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td>Tennessee</td>
<td>6 to 18</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Texas</td>
<td>6 to 19</td>
<td>5</td>
<td>35</td>
</tr>
<tr>
<td>Utah</td>
<td>6 to 18</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Vermont</td>
<td>6 to 16 ²²</td>
<td>5</td>
<td>—</td>
</tr>
<tr>
<td>Virginia</td>
<td>5 to 18</td>
<td>5</td>
<td>20</td>
</tr>
<tr>
<td>Washington</td>
<td>8 to 18</td>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td>West Virginia</td>
<td>6 to 17</td>
<td>5</td>
<td>22</td>
</tr>
<tr>
<td>Wisconsin</td>
<td>6 to 18</td>
<td>4</td>
<td>20</td>
</tr>
<tr>
<td>Wyoming</td>
<td>7 to 16 ²⁵</td>
<td>5</td>
<td>21</td>
</tr>
</tbody>
</table>
Not available. In this state, local education agencies determine their maximum or minimum age, or the information is not available in the statute.

In Alabama, the parent or legal guardian of a five-year-old child may opt out of enrolling their child by notifying the local board of education, in writing, that the child will not be in school until he or she is 7 years old.

In Alabama's city school systems, students are entitled to admission until age 19.

Alaska requires that students attend until they are 18 or complete 12th grade.

In Arizona, students must attend until they are 16 or complete 10th grade.

In California, no school district may receive school district appropriations for kindergarten or any of the 1st to 12th grades, inclusive, since their 18th birthday.

In Connecticut, the parent of a four-year-old child may opt out of enrolling their child until he or she is 7 by signing an option form.

In District of Columbia students who are at least 5 years old by September 30 are eligible for enrollment in the full-time public school program. Students who are 4 years old by September 30 are eligible for the pre-kindergarten program.

In Illinois, compulsory attendance is denied to any child 10 years of age or older who has dropped out of school and who cannot, because of age and lack of credits, attend classes during the normal school year and graduate before he or her 21st birthday.

In Iowa, children enrolled in preschool programs 4 years old on or before September 15 are considered to be of compulsory attendance age.

In Kansas, parents have access to an education if they enroll in a public school. However, school districts are not required to provide educational services in a regular school setting to anyone who does not reach 19 years of age and who is not currently enrolled in a school district. If a school district elects not to provide educational services in a regular school setting, the district must offer parents educational services in an alternative setting or program.

In Louisiana, admission must be granted to any student who is 19 years of age or younger on September 30 or 20 years old on September 30 and has sufficient course credits that he or she will be able to graduate within one school year of admission or reentry.

In Maine, students must be at least 5 years old before October 15, or 4 years old by October 15 if they are enrolled in a public preschool program prior to kindergarten (where available).

Each school committee in Massachusetts establishes its own minimum age for school attendance, provided that it is not older than mandatory minimum age established by the state.

In Missouri, attendance is required until 17 or the completion of 16 credits toward high school graduation.

In Nevada, students may attend a comprehensive public school until age 21; or, from age 18, they may attend an adult high school program. Their education must be for the purpose of adult education.

In New York, the boards of education in the city of Syracuse, New York City, Rochester, Utica, and Buffalo school districts are authorized to require children who are 6 years old on or before December 1 to attend kindergarten unless the parents cease to enroll their child until the following September, or the child is enrolled in a non-public school or home school program.

The board of education in any Pennsylvania school district may establish kindergarten programs for children between the ages of 4 and 8.

In Rhode Island, the compulsory age is 16 if a student has an alternative learning plan for obtaining a high school diploma or its equivalent.

Although some Rhode Island districts allow students to complete the school year after they turn 21, this practice is not universal and not required.

In South Carolina, individuals older than 21 years old may attend night schools.

In South Dakota, the compulsory age limit is 16 if a child succeeds in a general education development test preparation program that is school-based or in which a school contracts, and the child successfully completes the test or reaches the age of 18.

In Wyoming, students are entitled to attend school until they are 16 or complete 10th grade.

# Appendix D: Cyber.org 9-12 Cybersecurity Learning Standards

<table>
<thead>
<tr>
<th>Core Concept</th>
<th>Sub concept</th>
<th>Topic</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computing Systems (CS)</td>
<td>Network Communication (COMM)</td>
<td>9-12.CS.COMM</td>
<td>Explain layers within the OSI Networking Model.</td>
</tr>
<tr>
<td></td>
<td>Network Components (COMP)</td>
<td>9-12.CS.COMP</td>
<td>Create a diagram of a network utilizing appropriate network components.</td>
</tr>
<tr>
<td></td>
<td>Cloud Computing (CC)</td>
<td>9-12.CS.CC</td>
<td>Evaluate the risks and benefits of cloud computing.</td>
</tr>
<tr>
<td></td>
<td>Protocols (PROT)</td>
<td>9-12.CS.PROT.1</td>
<td>Compare and contrast the ports and protocols used for different services available.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9-12.CS.PROT.2</td>
<td>Identify the risks associated with the different services available online.</td>
</tr>
<tr>
<td></td>
<td>Data Loss (LOSS)</td>
<td>9-12.CS.LOSS</td>
<td>Develop a plan for risk mitigation that implements redundancy.</td>
</tr>
<tr>
<td>Digital Citizenship (DC)</td>
<td>Hardware Hardware Components (HARD)</td>
<td>9-12.CS.HARD</td>
<td>Identify methods of mitigating risk associated with connecting devices.</td>
</tr>
<tr>
<td></td>
<td>Internet of Things (IOT)</td>
<td>9-12.CS.IOT</td>
<td>Analyze the vulnerabilities of the Internet of Things devices.</td>
</tr>
<tr>
<td></td>
<td>Operating Systems (OS)</td>
<td>9-12.CS.OS</td>
<td>Create a plan for hardening an operating system.</td>
</tr>
<tr>
<td>Software</td>
<td>Software Updates (SOFT)</td>
<td>9-12.CS.SOFT</td>
<td>Compare the advantages and disadvantages of patching systems in real time.</td>
</tr>
<tr>
<td></td>
<td>Programming and Scripting (PROG)</td>
<td>9-12.CS.PROG</td>
<td>Describe the role of scripting in cyber-attacks and cyber defense.</td>
</tr>
<tr>
<td></td>
<td>Applications (APPS)</td>
<td>9-12.CS.APPS</td>
<td>Discuss how software that exists on and across various platforms can be used to monitor, collect, and analyze information from those platforms.</td>
</tr>
<tr>
<td>Online Safety</td>
<td>Cyberbullying (CYBL)</td>
<td>9-12.DC.CYBL</td>
<td>Prepare a plan to raise awareness of the effects of cyberbullying.</td>
</tr>
<tr>
<td>Category</td>
<td>Topic</td>
<td>Details</td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Digital Footprint (FOOT)</td>
<td>9-12.DC.FOOT</td>
<td>Examine the implications of both positive and negative digital footprints.</td>
<td></td>
</tr>
<tr>
<td>Personally Identifiable Information (PII)</td>
<td>9-12.DC.PPI.1</td>
<td>Explain the importance of social identity and the implications of online activity regarding private data, long-term career impacts, and the permanence of digital data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>9-12.DC.PPI.2</td>
<td>Explain the individual risks of a data breach to an organization housing personal data.</td>
<td></td>
</tr>
<tr>
<td>Ethics</td>
<td>Threat Actors (THRT)</td>
<td>9-12.DC.THRT Analyze the motives of threat actors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ethical Integrity (ETH)</td>
<td>9-12.DC.ETH Discuss the role that cyber ethics plays in current society.</td>
<td></td>
</tr>
<tr>
<td>Policy and Legal Issues</td>
<td>Rules, Laws, and Regulations (LAW)</td>
<td>9-12.DC.LAW Compare and contrast local, state, federal, and international cyber laws and regulations for individuals and businesses.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intellectual Property (IP)</td>
<td>9-12.DC.IP Debate the importance of intellectual property laws.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Usage and User Agreements (AUP)</td>
<td>9-12.DC.AUP Differentiate between the various agreements that protect individuals and organizations in their digital environments.</td>
<td></td>
</tr>
<tr>
<td>Security (SEC)</td>
<td>CIA TRIAD (CIA)</td>
<td>9-12.SEC.CIA Explain various interactions between the CIA Triad and the three states of data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access Control (ACC)</td>
<td>9-12.SEC.ACC Compare and contrast the concepts presented by access control principles, access control modules, and the principle of least privilege access.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Security (DATA)</td>
<td>9-12.SEC.DATA Formulate a plan to apply security measures to protect data in all three states.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Threats and Vulnerabilities (INFO)</td>
<td>9-12.SEC.INFO Distinguish the different types of attacks that affect information security for individuals and organizations.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cryptography (CRYP)</td>
<td>9-12.SEC.CRYP Analyze how modern advancements in computing have impacted encryption.</td>
<td></td>
</tr>
<tr>
<td>Network Security</td>
<td>Authentication (AUTH)</td>
<td>9-12.SEC.AUTH Evaluate authentication and authorization methods and the risks associated with failure.</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Securing Network Components (COMP)</td>
<td>9-12.SEC.COMP Evaluate Defense in Depth strategies that can protect simple networks.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Threats and Vulnerabilities (NET)</td>
<td>9-12.SEC.NET Analyze the different types of attacks that affect network security.</td>
<td></td>
</tr>
<tr>
<td>Physical Security</td>
<td>Threats and Vulnerabilities (PHYS)</td>
<td>9-12.SEC.PHYS Analyze the different types of attacks that affect physical security.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security Controls (CTRL)</td>
<td>9-12.SEC.CTRL Justify the use of Defense in Depth and the need for physical access controls.</td>
<td></td>
</tr>
</tbody>
</table>
## Appendix E: Teach Cyber Cybersecurity Curriculum Guidelines

<table>
<thead>
<tr>
<th>Big Idea</th>
<th>Enduring Understanding</th>
<th>Learning Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ethics</strong></td>
<td>1.1: Social goals reflect the foundational values held by society; these core societal values are reflected in cybersecurity choices.</td>
<td>1.1.1: Students will analyze online and offline behaviors in societies (themselves, peers, families, communities, and countries) and deduce the values that govern behaviors.</td>
</tr>
<tr>
<td></td>
<td>1.2: Ethical reflection and judgement are required in considering the potential harms, benefits, and trade-offs involved in cybersecurity.</td>
<td>1.2.1: Students will discuss how cybersecurity can significantly impact the quality of people’s lives both positively and negatively.</td>
</tr>
<tr>
<td></td>
<td>1.3: Cybersecurity practices are highly complex and variable causing tensions between what the ethical duties are, to whom the ethical concern should be considered, and whose interests should be invested in protecting.</td>
<td>1.3.1: Students will explore the tensions that exist between transparency, autonomy, resilience, and security.</td>
</tr>
<tr>
<td></td>
<td>2.1: Cybersecurity relies on confidentiality, integrity, and availability (the CIA triad).</td>
<td>2.1.1: Students will evaluate methods of keeping information secret from those whom the information should be kept secret.</td>
</tr>
<tr>
<td></td>
<td>2.2: The simpler you can make the design or implementation of a system, the better you can check whether it can be exploited.</td>
<td>2.2.1: Students will describe the principle of simplicity, which is about ensuring that systems are easy to understand, maintain and test to be more secure.</td>
</tr>
<tr>
<td><strong>Establishing Trust</strong></td>
<td></td>
<td>2.1.2: Students will demonstrate that integrity involves trust and credibility.</td>
</tr>
<tr>
<td></td>
<td>2.1.3: Students will evaluate methods of protecting information and information systems from disruption and destruction.</td>
<td>2.2.2: Students will use the principle of abstraction to represent complicated...</td>
</tr>
</tbody>
</table>
1. concepts more simply and to allow solutions to be transferred to other contexts.

2.2.3: Students will apply the principle of minimization by decreasing the number of ways in which attackers can exploit a program or device.

2.3: The more you restrict access, processes, resources, and users based on policy, the more secure the system.

2.3.1: Students will give examples of the principle of domain separation, which allows for the enforcement of rules governing the entry and use of domains by entities outside the domain.

2.3.2: Students will explain that the principle of process isolation prevents tampering or interference from / by other processes.

2.3.3: Students will explain the importance of encapsulating resources, i.e., creating well-defined interfaces around resources to set rules for how the resources should interact.

2.3.4: Students will define the principle of least privilege, which is about differentiating among types of access control (mandatory, role-based, discretionary, and rule-based access controls) and analyzing which to use for selective restriction of access to a place or other resource.

2.3.5: Students will break down how the principle of layering is a strategy for slowing down an attack because the attacker must conquer each layer before moving on to the next.

2.3.6: Students will know that the principle of data hiding is about allowing only necessary aspects of a data structure or a record to be observed or accessed.

2.3.7: Students will recognize that cybersecurity often applies to a system that consists of individual self-sufficient components and the overall security is dependent on the security prosperities of the components.

2.3.8: Students will define the principle of fail-safe defaults, which restricts how
<table>
<thead>
<tr>
<th>Ubiquitous Connectivity</th>
<th>Data Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2.4:</strong> Identifying and questioning assumptions is a key part of making a system more secure.</td>
<td><strong>4.1:</strong> Data security deals with the integrity of the data, i.e., the protection from corruption or errors; the privacy of data; and data confidentiality, i.e., it being accessible to only those who have access privilege to it.</td>
</tr>
<tr>
<td><strong>2.4.1:</strong> Given a scenario, students will identify the assumptions made in the design of the system, evaluate their impact on security, and consider how different assumptions change the security.</td>
<td><strong>4.1.1:</strong> Students will analyze existing data security concerns and assess methods to overcome those concerns.</td>
</tr>
<tr>
<td><strong>3.1:</strong> The Internet is a large globally distributed network that is divided into layers, governed by protocols, and connects a wide variety of devices.</td>
<td><strong>4.2:</strong> Data security uses non-technical and technical controls and techniques to protect data that is being processed, transmitted, and stored.</td>
</tr>
<tr>
<td><strong>3.1.1:</strong> Students will explain how devices use layers to communicate across the Internet and describe the purposes of the layers.</td>
<td><strong>4.2.1:</strong> Students will compare data protection legislation, policies, and procedures that have been or are being introduced all over the world to protect personal data.</td>
</tr>
<tr>
<td><strong>3.1.2:</strong> Students will explain how standards and protocols allow different types of devices to communicate.</td>
<td><strong>4.2.2:</strong> Students will identify physical controls that are used to secure data.</td>
</tr>
<tr>
<td><strong>3.2:</strong> The Internet provides a large attack surface, which offers efficiencies or economies of scale for adversaries.</td>
<td><strong>4.2.3:</strong> Students will evaluate and recommend technical controls that can be used to secure data.</td>
</tr>
<tr>
<td><strong>3.2.1:</strong> Students will analyze how the connected nature of the Internet allows an adversary to reach many devices.</td>
<td><strong>4.3:</strong> Cryptography techniques are necessary to keep data</td>
</tr>
<tr>
<td><strong>3.2.2:</strong> Students will identify and predict the outcomes of security vulnerabilities at the physical / link layer, the network layer, the transport layer, and the application layer.</td>
<td><strong>4.3.1:</strong> Students will define cryptography and explain how it is used in data security.</td>
</tr>
<tr>
<td><strong>3.2.3:</strong> Students will identify and distinguish between the purposes of network security devices and technology.</td>
<td><strong>4.3.2:</strong> Students will understand and apply cryptographic techniques to protect data.</td>
</tr>
<tr>
<td>Private and Secure</td>
<td>4.3.2: Students will practice symmetric cryptosystems to send a message and explain how they work.</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Evolve with Changes in Technology</td>
<td>5.1: Systems consist of a combination of hardware and software that together achieve some objective and security requires integration of both.</td>
</tr>
<tr>
<td>5.2: Hardware security protects the machine and peripheral hardware from theft and from electronic intrusion and damage.</td>
<td>5.1.2: Students will convey that computer hardware refers to the physical parts of a computer and related devices.</td>
</tr>
<tr>
<td>5.3: Security vulnerabilities in software are weaknesses in a system’s design, implementation, or operation and management that could be exploited to violate the system’s security policy.</td>
<td>5.2.3: Students will describe the process of developing secure hardware and validating that it is secure through its lifecycle.</td>
</tr>
<tr>
<td>5.4: Software and Hardware (or Systems) are everywhere which increasingly makes it foundational in civilization.</td>
<td>5.3.1: Students will describe common security related software vulnerabilities.</td>
</tr>
<tr>
<td>5.4.1: Students will identify historical consequences of software and hardware vulnerabilities, e.g., power outages, death, theft of trade secrets from other sovereign nations.</td>
<td>5.3.3: Students will describe the process of validating that software remains secure through its lifecycle.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Adversarial Thinking</th>
<th>6.1: Adversity comes from anyone or anything where the result differs from that intended by the system designer and user.</th>
<th>6.1.1: Students will explain how cybersystems are complex systems.</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1.2: Students will explain how complexity impacts the failure of cybersystems.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 6.1: System Components and Cybersecurity

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>6.1.3:</strong></td>
<td>Students will identify and explain how different system components impact the cybersecurity of a system design.</td>
<td></td>
</tr>
<tr>
<td><strong>6.1.4:</strong></td>
<td>Students will understand how social behaviors and human factors impact the cybersecurity of system design.</td>
<td></td>
</tr>
</tbody>
</table>

### 6.2: Adversarial Thinking

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>6.2.1:</strong></td>
<td>Students identify the ways in which natural events and unintentional errors can cause a system to fail.</td>
<td></td>
</tr>
<tr>
<td><strong>6.2.2:</strong></td>
<td>Students will explain how intentional attacks can adapt to defenses and cause a system to fail.</td>
<td></td>
</tr>
<tr>
<td><strong>6.2.3:</strong></td>
<td>Students will analyze how the cybersecurity attack lifecycle / kill chain is essential to adversarial thinking.</td>
<td></td>
</tr>
</tbody>
</table>

### Risk

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>7.1:</strong></td>
<td>Cybersecurity risk is a measure of the potential damage or loss a vulnerability could cause weighted against the likelihood an adversary will exploit the vulnerability.</td>
<td></td>
</tr>
<tr>
<td><strong>7.1.1:</strong></td>
<td>Students will be able to differentiate between threats, vulnerabilities, and attacks.</td>
<td></td>
</tr>
<tr>
<td><strong>7.1.2:</strong></td>
<td>Students will be able to identify and prioritize the protection of information assets.</td>
<td></td>
</tr>
<tr>
<td><strong>7.1.3:</strong></td>
<td>Students will create a threat model and evaluate the trade-offs associated with defending against different threat sources.</td>
<td></td>
</tr>
<tr>
<td><strong>7.1.4:</strong></td>
<td>Students will be able to conduct standard security testing and assessments.</td>
<td></td>
</tr>
<tr>
<td><strong>7.1.5:</strong></td>
<td>Students will understand the trade-offs between cybersecurity benefits and the total cost of cybersecurity protections.</td>
<td></td>
</tr>
</tbody>
</table>

### 7.2: Cybersecurity Risk Factors

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>7.2.1:</strong></td>
<td>Students will be able to explain how cyberspace is a very complex system of cybersystems that include hardware, software, social, economic, and political components.</td>
<td></td>
</tr>
<tr>
<td><strong>7.2.2:</strong></td>
<td>Students will be able to describe how the presence of an adversary necessitates that cybersecurity risk is emergent and complex.</td>
<td></td>
</tr>
<tr>
<td><strong>7.2.3:</strong></td>
<td>Students will be able to explain how the logical malleability of software and hardware can allow an adversary to change a system to meet the adversary’s...</td>
<td></td>
</tr>
<tr>
<td>Implications</td>
<td>7.2.4: Students will be able to explain how the decentralized and dynamic nature of networked systems create the potential for a system to fail or behave incorrectly due to a component the designer didn’t even know existed.</td>
<td></td>
</tr>
</tbody>
</table>
| 8.1: Cybersecurity shapes and is shaped by significant historical ideas and events. | 8.1.1: Students will summarize and interpret the impact of cybersecurity events on the evolution of the field.  
8.1.2: Students will explain how the idea of the open internet led us to new innovations that impact our daily lives and our security. |
| 8.2: Cybersecurity is global, transcending traditional boundaries, and is always evolving. | 8.2.1: Students will describe how political ideologies, economic structures, social organizations, and cultural perceptions that impact cybersecurity.  
8.2.2: Students will analyze how privacy concerns vary greatly regarding societies, age, and socio-economic status. |
| 8.3: Measuring the economic value of cybersecurity is often an indirect process that relies on risk management trade-offs rather than direct benefits. | 8.3.1: Students will explain how misaligned incentives encourage businesses to under invest in cybersecurity.  
8.3.2: Students will explain how economic forces influence the cybersecurity choices made by service providers and service designers.  
8.3.3: Students will describe how economics shape the decisions of consumers. |
## Appendix F: RING Curriculum

<table>
<thead>
<tr>
<th>Unit</th>
<th>Graphic Organizers &amp; Viewing Guides</th>
<th>Activities and Labs</th>
<th>Reviews and Resources</th>
<th>Assessments</th>
</tr>
</thead>
</table>
| Unit 0: Introduction | • Vocabulary Practice 0.1 | • Cybersecurity Careers Quiz  
• Cybersecurity Careers  
• Demonstration: OSINT (Teacher Only)  
• EXIF Extraction | • Quizlet  
• Kahoot | |
| Unit 1: Ethics | • Vocabulary Practice:  
1.1 and 1.2  
• Viewing Guides:  
How Facebook Tracks Your Data (Student)  
The First Computer Virus  
Types of Hackers Explained  
STAR | • Impact of Values  
• Cyber Institute Code of Ethics  
• Code of Ethics Pledge  
• How Organizations use Collected Data  
• Ethics Drag and Drop  
• Reaper vs Creeper  
• Design vs Use  
• Insecure Security Resources  
• Hat the Hacker  
• Black Hat Crimes Will Cost You Time | • Quizlet 1  
• Kahoot 1  
• Quizlet 1.2  
• Kahoot 1.2 | • Project: In the Court of Ethics  
• Ethics Assessment Items |
| Unit 2: Establishing Trust | • Vocabulary Practice:  
2.2  
• Graphic Organizer:  
Classify the CIA Triad  
Cybersecurity Principles Examples  
Inside a Computer  
Pick Your Access Control  
• Viewing Guide:  
Command Line Interfaces  
Economy of Mechanism  
Linux 4 Permissions  
Network Security Defense in Depth  
Vulnerabilities and Exploits  
What is Encapsulation?  
| • Activity:  
Caesar Cipher  
Changing Privilege  
Hiding Files  
Linux Commands  
Extension Activity:  
Make It@Home: Scytale  
Modern Encryption  
Spam Mimic  
MIT Terminus Command Line Game  
The Missing Semester of Your CS Education  
E-Mates | • Quizlet 2.1  
• Kahoot 2.1  
• Caesar Cipher Demo  
• Steganography Online Tool  
• Quizlet 2.2  
• Kahoot 2.2  
• Cybersecurity First Principles  
• Fort Knox ITs Security  
• Kahoot Cybersecurity Principles |
| Unit 3: Ubiquitous Connectivity | Vocabulary Practice: 3.1, 3.2, and 3.3  
Graphic Organizers:  
How Does Information Travel?  
Layers of Cyberspace  
Protocols  
The Dark Side of the Web  
Clients, Servers & Hosts  
HIDS vs NIDS  
Navigating Networks  
Space Travel  
Types of Cloud Services  
Types of Networks  
Viewing Guides:  
A Packet’s Tale  
How Big is the Internet  
How Computers Work  
Packet Header  
The Internet Defined  
What is a Server?  
What is DNS?  
6 Layers Deep  
Application Layer  
Inside a Google Data Center  
IPv4 vs IPv6  
The OSI Model  
Switches and Routers  
TCP/IP Model  
TCP vs UDP  
What is a DDoS Attack  | Activity:  
ABC: What is the Internet  
Bits & Bytes  
Capturing the Net  
CS Unplugged  
DDoS Attacks  
Hacking Websites  
Location, Location, Location  
MAC Address  
Networks, Hubs, Switches, & Routers  
Network Technologies  
Server Sleuth Activity  
Permission Impossible  
Netstat Lab  
Traceroute Lab  
VM Introduction / NetLab  
Extension Activity:  
Binary Numbers  
Microsoft’s Underwater Data Center  
Hexadecimal  
The Internet  
How to Figure Out What Country Your Data is Stored In  | Quizlet 3.1  
Kahoot 3.1  
Flippy Do  
Binary Blitz Numbers Game  
IP Header Format  
Cybersecurity Interactive  
What is IP?  
Spoofing and DoS Attacks |
<table>
<thead>
<tr>
<th>Unit 4: Data Security</th>
<th>Vocabulary Practice:</th>
<th>Activity:</th>
<th>Quizlet 4.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4.1, 4.2, and 4.3</td>
<td>Asymmetric Practice</td>
<td>Kahoot 4.1</td>
</tr>
<tr>
<td></td>
<td>Graphic Organizers:</td>
<td>Broken Authentication</td>
<td>Quizlet 4.2</td>
</tr>
<tr>
<td></td>
<td>Asymmetric Crypto</td>
<td>Cryptography Warm-up Intro</td>
<td>Kahoot 4.2</td>
</tr>
<tr>
<td></td>
<td>Public and Private</td>
<td>Data Defense</td>
<td>Quizlet 4.3</td>
</tr>
<tr>
<td></td>
<td>keys</td>
<td>Data Security Concerns</td>
<td>Kahoot 4.3</td>
</tr>
<tr>
<td></td>
<td>Viewing Guides:</td>
<td>Physical Controls</td>
<td>Interactive</td>
</tr>
<tr>
<td></td>
<td>Asymmetric Encryption</td>
<td>Red vs Blue</td>
<td>Caesar Cipher</td>
</tr>
<tr>
<td></td>
<td>Passwords and Hash</td>
<td>Security Life Cycle</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Functions</td>
<td>Session Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Privacy and Data</td>
<td>Situation States</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protection</td>
<td>Symmetric Cryptosystems</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RSA Encryption</td>
<td>Technical Controls</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Algorithm</td>
<td>The Man Not the Salad</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dressing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Transposition Cipher</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Two Factor Authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>E-mates:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Digital Signature</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unit 5: Introduction to Python Programming</th>
<th>Vocabulary:</th>
<th>Activity:</th>
<th>Quizlet 5.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5.1, 5.2, 5.3</td>
<td>High and Low</td>
<td>Quizlet 5.2</td>
</tr>
<tr>
<td></td>
<td>Graphic Organizer:</td>
<td>New Skill =</td>
<td>Quizlet 5.3</td>
</tr>
<tr>
<td></td>
<td>Interpreted / Compiled</td>
<td>‘Variable Practice’</td>
<td>Acadly</td>
</tr>
<tr>
<td></td>
<td>Viewing Guide:</td>
<td>User-Defined Functions</td>
<td>Google Translate</td>
</tr>
<tr>
<td></td>
<td>Basic Data Types</td>
<td>Truth Table Sort</td>
<td>Translate</td>
</tr>
<tr>
<td></td>
<td>Immutable Data Types</td>
<td></td>
<td>Online GDB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unit 5: Introduction to Python Programming</th>
<th>Activity:</th>
<th>Quizlet 5.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>High and Low</td>
<td>Quizlet 5.2</td>
</tr>
<tr>
<td></td>
<td>New Skill =</td>
<td>Quizlet 5.3</td>
</tr>
<tr>
<td></td>
<td>‘Variable Practice’</td>
<td>Acadly</td>
</tr>
<tr>
<td></td>
<td>User-Defined Functions</td>
<td>Google Translate</td>
</tr>
<tr>
<td></td>
<td>Truth Table Sort</td>
<td>Online GDB</td>
</tr>
</tbody>
</table>
| Unit 6: System Security | Vocabulary:  
- 6.1 and 6.2  
- SSDLC  
- Impacting Integrity  
- Secure Coding Principals  
- Unavailable  
- Side Channel Classes  
- Breaking the Chain  
- Viewing Guide:  
  - How Computers Work  
  - GTS/HMI  
  - What is Patching?  
  - What is Command Injection?  
  - Cracking Websites  
  - Cyber Physical Systems | Activity:  
- Hardware Spy  
- Component Connection  
- Fail Safes  
- Hardware Security Guidelines  
- Hardware Soft-Spots  
- Embedded Software  
- SDLC  
- Common Weakness Enumeration  
- Software Vulnerability Examples  
- Injection Attacks  
- Cyber Physical Systems  
- SCADA  
- Unfortunate Consequences  
- Dynamic Analysis  
- Static Analysis  
- E-mate:  
  - Code injection  
  - OS Command Injection  
  - Malware Types, APT | Quizlet 6.1  
Kahoot 6.1  
Quizlet 6.2  
Kahoot 6.2  
Hack Math |
<table>
<thead>
<tr>
<th>Zero-Day Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab:</td>
</tr>
<tr>
<td>Buffer Overflow</td>
</tr>
<tr>
<td>Activity:</td>
</tr>
<tr>
<td>Pwned</td>
</tr>
<tr>
<td>Rating Hacks</td>
</tr>
<tr>
<td>Two Truths and a Lie</td>
</tr>
<tr>
<td>Keep a Business Running</td>
</tr>
<tr>
<td>E-mate:</td>
</tr>
<tr>
<td>Threat Actors</td>
</tr>
<tr>
<td>Social Engineering</td>
</tr>
<tr>
<td>Social Engineering Psychological Tactics</td>
</tr>
<tr>
<td>Phishing Mystery</td>
</tr>
<tr>
<td>Pentesting</td>
</tr>
<tr>
<td>Project:</td>
</tr>
<tr>
<td>Security Awareness Campaign</td>
</tr>
<tr>
<td>Security Policies</td>
</tr>
<tr>
<td>Quizlet 7.1</td>
</tr>
<tr>
<td>Kahoot 7.1</td>
</tr>
<tr>
<td>Quizlet 7.2</td>
</tr>
<tr>
<td>Kahoot 7.2</td>
</tr>
<tr>
<td>Quizlet 7.3</td>
</tr>
<tr>
<td>Kahoot 7.3</td>
</tr>
<tr>
<td>Columbus State Social Engineering Quiz</td>
</tr>
<tr>
<td>Real or Phish?</td>
</tr>
<tr>
<td>Change Management Exercise</td>
</tr>
<tr>
<td>Cyber Kill Chain</td>
</tr>
<tr>
<td>FBI IC3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unit 7: Adversarial Thinking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vocabulary:</td>
</tr>
<tr>
<td>7.1, 7.2, and 7.3</td>
</tr>
<tr>
<td>Graphic Organizer:</td>
</tr>
<tr>
<td>Adversaries</td>
</tr>
<tr>
<td>Viewing Guide:</td>
</tr>
<tr>
<td>Vulnerability Scanning</td>
</tr>
<tr>
<td>Unit 8: Risk</td>
</tr>
<tr>
<td>Vocabulary:</td>
</tr>
<tr>
<td>8.1, 8.2, and 8.3</td>
</tr>
<tr>
<td>Graphic Organizer:</td>
</tr>
<tr>
<td>Threats and Actors</td>
</tr>
<tr>
<td>Data Breach vs Data Leak</td>
</tr>
<tr>
<td>Threats, Vulnerabilities, and Attacks</td>
</tr>
<tr>
<td>Hackers and Cyber Attacks</td>
</tr>
<tr>
<td>NIST Framework</td>
</tr>
<tr>
<td>Viewing Guide:</td>
</tr>
<tr>
<td>Cybersecurity Crash Course</td>
</tr>
<tr>
<td>Activity:</td>
</tr>
<tr>
<td>User Security Awareness Game</td>
</tr>
<tr>
<td>OWASP Top 10</td>
</tr>
<tr>
<td>NVD Research</td>
</tr>
<tr>
<td>The Future of Cybersecurity Article</td>
</tr>
<tr>
<td>Sort the Asset</td>
</tr>
<tr>
<td>Complex System Behaviors</td>
</tr>
<tr>
<td>NSA Top 10 Mitigation Strategies</td>
</tr>
<tr>
<td>The Importance of Planning</td>
</tr>
<tr>
<td>Vulnerability Scanning Tools</td>
</tr>
<tr>
<td>Quizlet 8.1</td>
</tr>
<tr>
<td>Kahoot 8.1</td>
</tr>
<tr>
<td>Quizlet 8.2</td>
</tr>
<tr>
<td>Kahoot 8.2</td>
</tr>
<tr>
<td>Quizlet 8.3</td>
</tr>
<tr>
<td>Kahoot 8.3</td>
</tr>
<tr>
<td>Prevent Vulnerabilities</td>
</tr>
<tr>
<td>Targeted Attacks</td>
</tr>
<tr>
<td>BPA Oil Spill Article</td>
</tr>
<tr>
<td>5 Steps to Mitigate Legal Risks in Business Article</td>
</tr>
<tr>
<td>What are Complex Systems? Discussion</td>
</tr>
<tr>
<td>Unit 9: Implications</td>
</tr>
<tr>
<td>----------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Graphic Organizer:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Activity:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Quizlet 9.1</td>
</tr>
<tr>
<td>Quizlet 9.2</td>
</tr>
<tr>
<td>Quizlet 9.3</td>
</tr>
<tr>
<td>Quizlet 9.4</td>
</tr>
<tr>
<td>Quizlet 9.5</td>
</tr>
<tr>
<td>Quizlet 9.6</td>
</tr>
<tr>
<td>Quizlet 9.6</td>
</tr>
<tr>
<td>National Cyber Security Index Map</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>• Misaligned</td>
</tr>
<tr>
<td>Incentives</td>
</tr>
<tr>
<td>• Viewing</td>
</tr>
<tr>
<td>Guide:</td>
</tr>
<tr>
<td>• Interplanetary</td>
</tr>
<tr>
<td>Internet</td>
</tr>
<tr>
<td>• Political</td>
</tr>
<tr>
<td>Ideologies</td>
</tr>
<tr>
<td>• Nigerian</td>
</tr>
<tr>
<td>Prince</td>
</tr>
<tr>
<td>Scam</td>
</tr>
<tr>
<td>• US Cyber</td>
</tr>
<tr>
<td>Infrastructure</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Appendix G: RING Curriculum Artifacts

Lesson Plan Example

Day 1: 1.1 (Slides 1-13)

Monday, August 10th, 2020

RING
Day 1: 1.1 (Slides 1-13)

Learning Objectives
1.1.1a EK Societies are groups of individuals characterized by common interests/values that are perpetuated by persistent social interaction. National Cryptologic Museum Foundation Cybersecurity
1.1.1b EK Cybersecurity ethics is an expression of values by the designers and users. National Cryptologic Museum Foundation Cybersecurity
1.1.1d EK Different communities and societies have different foundational social goals and values that impact their behaviors concerning technology. National Cryptologic Museum Foundation Cybersecurity
1.1 EU Social goals reflect the foundational values held by society; these core societal values are reflected in cybersecurity choices. National Cryptologic Museum Foundation Cybersecurity
1.1.1 LO Students will analyze online and offline behaviors in societies, i.e., themselves, peers, families, communities, and countries, and deduce the values that govern these behaviors. National Cryptologic Museum Foundation Cybersecurity

CAE KUs (None)

Lesson Delivery and Setup
Instructor will need a computer, access to the Internet, and a projector (or appropriate screen sharing software if virtual).
Student activities can be completed on paper or digitally.
Students will need access to the Internet for some activities.
Link to the slides:
https://docs.google.com/presentation/d/1ibJ62kDOY9ygSwk_Tc2j1AyskWRy0yCUHgppilPkQII/edit?usp=sharing

Procedures
Student objectives and big ideas are clearly defined and should be iterated when appropriate throughout the slide deck. Multiple graphic sources are available throughout the unit and should be referenced whenever available to reinforce the concepts being delivered. Activities for student practice and informal assessment will be available for key concepts and big ideas. Assignment requirements and parameters should be read to ensure student comprehension of the concepts and expectations.

**Warm-Up Activity**

Introduction to unit, ask students what they know about ethics. Ask about the relation between ethics and cybersecurity.

**Direct Instruction**

**Unit 1 Intro Slides (Slides 1-4):**
Introduce the unit with the title slide and discussion. Pose the question, "What are ethics?" to the class (answers will vary). Slide 3 introduces the vocabulary terms that will be covered and referenced throughout Section 1.1. Read the terms listed and explain that they will be explained more in-depth as they appear in the unit. Slide 4 introduces the Big Ideas for the unit. It is important for students to understand the purpose of the unit and the information that will be covered upon completion. Assign the Vocabulary Graphic Organizer Unit 1.1 linked in the Guided/Independent Practice section below.

Link to Quizlet: https://quizlet.com/_brs3ns?x=1qqt&i=3cpoah
Link to Kahoot: https://create.kahoot.it/details/58d9ceb1-a4ce-44df-b8be-3db8877c1660

**Ethics Unit 1.1 Title Slide - Quote for Discussion:**
Slide 5 is the title slide for Section 1.1. Slide 6 introduces the quote for discussion. Ask the students to read the quote before reading it to the class. Engage in a class-wide discussion with the following prompts:

*How might the quote tie into the discussion on ethics?*
*How are high levels of access considered a great responsibility?*
*What does Aiden Knowles mean by technology gatekeepers?*
*What does the quote mean?*

Continue by discussing the responsibility associated with high levels of access:
"Knowles then goes on to mention the great responsibility and high levels of access entrusted to professionals. Again, thinking back to Unit 0, how might being a ‘technological gatekeeper’ require trust?"
Ask the students to keep the quote in mind as you work through the unit.

**What is a Society?:**
Discuss the meaning of a society with the class. Students are likely to understand the meaning or concept of a society. Pose the question on the slide and allow time for student answers.

Possible answers may include:
Societal rules are guidelines we create collectively as a society. They are formed and maintained through interaction(s) and culture. Societal rules or guidelines we create collectively that distinguish between right and wrong.

Examples of societal norms:
Shake hands when meeting someone (pre-COVID).
Don’t eat off of another person’s plate without asking.
Always try to arrive on time for class or other appointments.

Vocabulary introduced on slide:
**Societies**: Groups of individuals with similar values and interests maintained through persistent social interaction.

Societal Norms and Ethics:
Discuss the relationship between societal rules and ethics. The societal rules (ethics) we set as a society influence what is and isn’t acceptable in cybersecurity. This can vary from one culture to another, as there are varying degrees of values in place based on beliefs and lifestyles. Pose the question, "How are societal ethics and cybersecurity ethics related?"

Possible answers may include:
Ethics apply to cybersecurity in similar ways to how they apply to day-to-day life. Cybersecurity is like a society of its own, and as such, it has ethical rules that are applicable to the practices.

Vocabulary introduced on slide:
**Ethics**: The set of values and rules we adhere to as defined by the societies in which we live.

The Influence of Culture on Technology (Slide 9):
Discuss the cultural influence(s) on technology usage, development, and advancement. Pose the question, "What do all of these things have in common?" in reference to the information and graphic sources provided.

Possible answers may include:
Speed
Convenience

The Influence of Culture on Technology (Slide 10):
Further discuss the cultural influence(s) on usage, development, and advancements in technology. Due to America's approach, we typically live lifestyles centered around speed and convenience. Further elaborate with the following points:
Culture has impacted the way we socialize through social media platforms.
Our culture has pushed for advancements in luxuries that other cultures may not value as much (the abundance of fast-food restaurants, for example).
The Influence of Culture on Technology (Slides 11-12):
Introduce the examples of how values and cultural differences impact technology.

The Impact of Values:
As stated in the previous slides, values impact the direction in which technology advances. In many other countries with different values, developers and designers often opt to create software, hardware, or other social media platforms that cater to their values. For example, users who hold certain political views may opt to use social media platforms or online threads that align with their opinions, rather than platforms or media sites that have differing opinions to their own. Users who value privacy may choose to only interact with technology that guarantees such or use a VPN to keep their interactions online discrete.

Possible answers may include:
Student answers are likely to vary greatly. They may include using technology that helps with time management and social media platforms. Offline behaviors may include being part of a family-oriented household unit that does activities together, eats meals together, etc.

Assign the Impact of Values Activity. In the directions to the assignment there is a link to a website (https://personalvalue.es/) that will help students get a better understanding of the values they hold and to what degree. Have them complete the questionnaire before answering the questions in the assignment.

Guided/Independent Practice

Slide 1, Vocabulary Graphic Organizer:
Vocabulary Graphic Organizer (Teacher): https://docs.google.com/document/d/1r3QMV1vxaZpvhsZ8T0y99nfc-0qcPhB3v4vb_CKOGY/edit?usp=sharing
Vocabulary Graphic Organizer (Student): https://docs.google.com/document/d/1QxY7ISpU3-uAazPX4t8G3ZAhnIzj8IftJtDSGJgffTU/edit?usp=sharing

Homework or Extension Activities
As an extension activity, encourage students to have a family member or friend complete the activity on slide 10 and compare the answers to their own.

Assessments
Teacher observation during lessons and participation (informal observations). The teacher should note whether student responses are appropriate for the line of questioning and whether participation is stagnant (which indicates lack of comprehension). Activity should be graded to formally assess student comprehension.
Slide Example

**Note to the instructor:**
Further discuss the cultural influence(s) on usage, development, and advancements in technology. Due to America’s approach to ethics, we typically live lifestyles centered around speed and convenience.

**Possible answers may include:**
- Culture has impacted the way we socialize through social media platforms and applications.
- Our culture has pushed for advancements in technology that other cultures may not value as much.

**Standard(s):**
- 1.1.M 1K Different communities and societies have different foundational societal goals and values that impact their behaviors concerning technology.
- 1.K.M 1K Social goals reflect the foundational values held by society. These core societal values are reflected in cybersecurity choices.

**Source(s):**
https://learnedinhisview.wordpress.com/2015/05/31/american-culture-assimilar-or-anomalous/

**Kahoot**

**Log into Kahoot!**
Log in to play this Kahoot and discover millions more you'll love!

<table>
<thead>
<tr>
<th>Questions (20)</th>
<th>Show answers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - Quiz</td>
<td>Groups of people characterized by common interests and values that are perpetuated by persistent social interaction.</td>
</tr>
<tr>
<td>2 - Quiz</td>
<td>The set of values and rules that we adhere to as defined by the societies in which we live.</td>
</tr>
<tr>
<td>3 - Quiz</td>
<td>Shared understandings, and formal doctrines that constrain actors’ interactions with one another.</td>
</tr>
<tr>
<td>4 - Quiz</td>
<td>An expression of values by designers and users in the institution of cybersecurity.</td>
</tr>
<tr>
<td>5 - Quiz</td>
<td>Criminals that use cybersecurity unfairly.</td>
</tr>
</tbody>
</table>
Quizlet

Unit 1.1: Ethics Vocabulary

Groups of people characterized by common interests and values that are perpetuated by persistent social interaction.

E-Mate

The McCumber Cube is a model framework created by John McCumber in 1991 used to establish and evaluate information security programs. This security model has three dimensions and looks like a Rubik’s cube.
## Vocabulary Practice: Ethics Pt. 1

**Quizlet**
See the following link for Quizlet practice: [https://quizlet.com/_9cz41r?x=1jqt&i=3h6had](https://quizlet.com/_9cz41r?x=1jqt&i=3h6had)

**Directions:** Write the definition for each vocabulary term in your own words. Then use the word in a sentence. After you have written the definition and sentence, rate your understanding of the word.

<table>
<thead>
<tr>
<th>Word</th>
<th>Definition</th>
<th>Picture</th>
<th>Sentence</th>
<th>Rate Your Understanding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Societies</td>
<td>Groups of people characterized by common interests and values that are perpetuated by persistent social interaction.</td>
<td><img src="image" alt="Societies" /></td>
<td></td>
<td>Answers may vary.</td>
</tr>
<tr>
<td>Ethics</td>
<td>The set of values and rules we adhere to as defined by the societies in which we live.</td>
<td><img src="image" alt="Ethics" /></td>
<td></td>
<td>Answers may vary.</td>
</tr>
<tr>
<td>Political Structures</td>
<td>The relation between institutions and how they interact with one another and the laws and norms they present.</td>
<td><img src="image" alt="Political Structures" /></td>
<td></td>
<td>Answers may vary.</td>
</tr>
<tr>
<td>Institution</td>
<td>Informal norms, shared understandings, and formal doctrines that constrain and prescribe actors' interactions with one another.</td>
<td><img src="image" alt="Institution" /></td>
<td></td>
<td>Answers may vary.</td>
</tr>
<tr>
<td>Code of Ethics</td>
<td>An expression of values by designers and users in the institution of cybersecurity.</td>
<td>Answers may vary.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethical Reflection</td>
<td>The act of considering the potential harms, benefits, and trade-offs involved in cybersecurity.</td>
<td>Answers may vary.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Graphic Organizer – Types of Cloud Services

Name: _______________________
Date: ________________________
Period/Block: ________________

### Types of Cloud Services – KEY

**Directions:** Fill out the following table regarding types of cloud services.

<table>
<thead>
<tr>
<th>Cloud Service</th>
<th>Graphic</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software as a Service (SaaS)</td>
<td><img src="cloud_icon.jpg" alt="Cloud Icon" /></td>
<td>Software as a Service (SaaS) is software or applications provided as a subscription or on a pay-as-you go basis. The software is located on external servers, with the user logging in to use it.</td>
<td>Google Docs or Dropbox</td>
</tr>
<tr>
<td>Desktop as a Service (DaaS)</td>
<td><img src="desktop_icon.jpg" alt="Desktop Icon" /></td>
<td>Desktop as a Service (DaaS) provides virtualized applications and desktop environments, allowing centralized configuration and management.</td>
<td>Amazon Workspaces</td>
</tr>
<tr>
<td>Platform as a Service (PaaS)</td>
<td><img src="platform_icon.jpg" alt="Platform Icon" /></td>
<td>Platform as a Service (PaaS) allows a way for developers to create customized applications. The servers, storage, and networking can be managed by the enterprise.</td>
<td>Windows Azure</td>
</tr>
<tr>
<td>Infrastructure as a Service (IaaS)</td>
<td><img src="infrastructure_icon.jpg" alt="Infrastructure Icon" /></td>
<td>Infrastructure as a Service (IaaS) provides servers, networks, operating systems, and storage. The client has control over the entire infrastructure, just as if the data center was provided locally.</td>
<td>Amazon Web Services</td>
</tr>
</tbody>
</table>
Activity – The Impact of Values

Name: _______________________
Date: ________________________
Period/Block: ________________

The Impact of Values

Directions: First, visit the following link and complete the personal values assessment: [https://personalvalu.es/](https://personalvalu.es/).
Upon completion of the assessment, answer the following questions to the best of your ability.

List your top five values:

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>2.</td>
<td>3.</td>
<td>4.</td>
<td>5.</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Which of your values impact the way you interact with your family and friends?</td>
<td></td>
</tr>
<tr>
<td>Which of your values impact your planned future career path?</td>
<td></td>
</tr>
<tr>
<td>Which of your values impact the technology you interact with?</td>
<td></td>
</tr>
<tr>
<td>Which of your values impact your online decisions and behaviors?</td>
<td></td>
</tr>
<tr>
<td>Which of your values impact your offline decisions and behaviors?</td>
<td></td>
</tr>
</tbody>
</table>
Viewing Guide – How Facebook Tracks Your Data

Name: _______________________
Date: _______________________
Period/Block: __________________

**Viewing Guide: How Facebook Tracks Your Data**

**Directions:** After watching the video, answer the following questions and fill in the blanks accordingly.

1. Facebook uses nearly ____100___ different data points to classify your interests and activities.

2. How can Facebook determine where you are?
   ___location services____

3. Facebook has partnerships with ____data brokers____ that collect information about people’s purchases.

4. How can Facebook tell if you are in a relationship or going through a break-up?
   ___Facebook monitors your likes and interactions___

5. True or False: Facebook gathers your personal information to predict your life outcomes.
Part I: Which is more important?

Directions: Read the following scenario and answer the questions that follow.

While not always to this degree, professionals must make similar decisions when faced with complex situations, for example:

Imagine you are an app developer for a large social media company that markets itself as offering 100% anonymity, and as a result, has the largest user base in many countries. During development, you notice that there have been multiple data breaches that have been quietly handled by your employer. The breaches have exposed thousands of users' private information including their addresses, jobs, and shopping habits to an unknown third-party. The vulnerability that was exploited is one that the company has known about for some time, yet they abstained from addressing it until after the attack had occurred. In this instance, you could go public with the knowledge; however, you would be violating the obligations you hold to your employer.

Before navigating the dilemma, it is important to understand what is most important to you, whether it be

- Security
- Trust
- Privacy
- Accountability
- Reputation
- Honesty
- Loyalty
- Success
- Etc.

When conducting ethical reflection, your values may conflict with those of the company you work for. In the above instance, the social media company quietly dealt with the situation without making the data breaches public.

Student answers on the activity can and will vary. Use best judgment to determine whether the answers are acceptable for the assignment or not.
Using the short list above, which values do you feel the company violated the most? Select three, and explain your reasoning:

<table>
<thead>
<tr>
<th>Company Values</th>
<th>Reasoning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy</td>
<td>The company violated privacy inherently due to the occurrence of the leak.</td>
</tr>
<tr>
<td>Honesty</td>
<td>The company violated honesty by not disclosing the leak to their users.</td>
</tr>
<tr>
<td>Accountability</td>
<td>The company violated accountability by trying to sweep the leak under the rug.</td>
</tr>
</tbody>
</table>

Why might the company's values prevent the company from disclosing the data breach?

The company markets itself as offering complete anonymity for its users. If the knowledge of several breaches got out, that would negatively impact their reputation.

By not disclosing the data breach, is the company acting unethically? Explain.

Yes. The company has an obligation to their user-base to share when breaches occur.

It is unethical for any company.
Note: Before making a decision, it is important to decide what values you hold, your obligations to your employer, and the ramifications of your actions.

In the above scenario, you are an employee at the social media company. As an employee, it is your obligation to hold the company’s best interest in high regard. By going against the company and disclosing the breach, you are running the risk of being fired or sued. You also face the possibility of difficulty obtaining future employment in your career field. How do you proceed?

Student answers will vary.

**Part II: Research**

**Directions:** Conduct research on the **Mossack Fonseca** law firm in relation to the leak. Use your research to answer the following questions. Cite your sources in the appropriate field beneath each question.

Does the law firm (Mossack Fonseca) hold any ethical responsibility for the leak? Why or why not?
Student answers may contain opinions. Mossack Fonseca does hold ethical responsibility for the successful leak.

Did Mossack Fonseca act ethically in their business practices? Why or why not?

They did not. Mossack Fonseca had many unethical dealings with arms dealers, and money laundering.

Source: website URL
Buffer overflows are classified as “bugs” in a program written in “memory unsafe” programming languages such as C or C++.

Note: C and C++ are considered memory unsafe, as they allow programmers a great deal of control over memory management.

Buffer overflow bugs from user input can often allow someone to knowingly or unknowingly overwrite some data in memory that they shouldn’t be allowed to.

In the activity, you will use the following blog post by Nagarro Security to better understand how buffer overflow occurs.
Part 1: Assembly Interaction

Assembly language is “raw machine code” as it is the lowest level programming language. The computer or device’s processor executes assembly instructions exactly as they are written. Click the RUN button to execute the program. We can see what happens when we execute the

\[
\text{mov \{register\}, \{value\}}
\]

1. What does the mov command do?

The mov command tells the processor to store (or "move") values into a register or memory address.

2. What happens to the register each time the mov instruction executes?

The register updates with the value specified in the mov instruction.

3. Use the table below to show the HEX values after the program executes:

<table>
<thead>
<tr>
<th>Register</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAX</td>
<td>0x00001337</td>
</tr>
<tr>
<td>RBX</td>
<td>0x00007331</td>
</tr>
<tr>
<td>RDI</td>
<td>0x00001995</td>
</tr>
</tbody>
</table>

Note: You may also click the STEP button to execute the program line by line.

Part 2: Stack
As we learned in Unit 5, the **stack** is a temporary place to store values in the memory (RAM). The data is stored and retrieved in predetermined increments determined by the type of operating system (OS) in use.

1. **Use the information in the blog to complete the table below:**

<table>
<thead>
<tr>
<th>System</th>
<th>Storage/Retrieval in bits</th>
<th>Storage/Retrieval in bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>64-bit System</td>
<td>64 bits</td>
<td>8 bytes</td>
</tr>
</tbody>
</table>

2. **What command is used to add or store data in the stack?**

   The push command is used, followed by the register name.

3. **What command is used to retrieve or fetch a value from the stack?**

   The pop command is used, followed by the register name.

4. **Why does the RSP decrease by 8 when the pop command is used?**

   The RSP decreases because the values in the stack reduce in size. The decrease is in 8-byte increments because the sample system is 64-bits.

5. **What do you observe when you run the program?**

   The RAX is set to the HEX value 0x13371337 and pushed into the stack before popping it into RDI.

---

**Part 3: RIP**

In addition to **RSP**, there is another **special register** known as **RIP**.

**RIP** always points to the memory address of the next instruction the process will execute. Unlike with **RSP**, the **RIP cannot be changed with the mov command**; instead, the **jmp** command must be used.
Note: In the image above, we can see how the jmp command is used in place of the mov command. The jmp command allows us to “jump” to different places in the program as needed.

RUN the program.

1. What can we observe in the flow of execution of the program?

The program jumps around depending on the command, for example: the jmp add1 command moves the program to the add1 module of the program. When the program jumps to "add2" 2 is added to the current value of RAX, when the program jumps to “add1”, 1 is added.

Another way to jump to another location in the code is to use the call instruction.

2. How does the call instruction work?+

The instruction pushes the address of the next instruction after the call instruction to stack, then jumps to the specific address.

3. How does the ret instruction work?

The ret instruction pops the last value on the stack and jumps (returns) to that address. This lets pieces of code act as functions that you can call and then return from when it's done and continue normal execution.

4. What can you observe from the stack when the program using nested calls is executed? Why?

The stack grows and shrinks as calls and returns are being executed.
## Appendix H: Cyber.org Cybersecurity Curriculum

<table>
<thead>
<tr>
<th>Unit</th>
<th>Lesson</th>
<th>Lab</th>
<th>Resource</th>
<th>Case Study</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux Basics</td>
<td>• 4.1.2 File Manipulation Tools</td>
<td>• Linux 101</td>
<td>• Syllabus Example</td>
<td>• Data Destruction</td>
</tr>
<tr>
<td></td>
<td>• 4.1.3 Shell and Shell Script Environments</td>
<td>• Linux 102</td>
<td>• Acceptable Use</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 4.1.1 Network Reconnaissance and Discovery Tools</td>
<td>• Iconfig</td>
<td>Possible</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 4.1.4 Packet Capture and Replay Tools</td>
<td>• Trace Route</td>
<td>Fun with Linux</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 4.1.8 Data Sanitization Tools</td>
<td>• TCPDump</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2.7.2 Data Destruction</td>
<td>• Wireshark</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Linux 101</td>
<td>• Data Sanitization</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Linux 102</td>
<td>• Autopsy</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Ifconfig</td>
<td>• Metadata</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Trace Route</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• TCPDump</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Wireshark</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Data Sanitization</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Autopsy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Metadata</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>• 4.2.1 Incident Response Process</td>
<td>• Passwords</td>
<td>• Incident Response</td>
<td></td>
</tr>
<tr>
<td>Basics</td>
<td>• 4.4.1 Post-Incident Mitigation Techniques</td>
<td>• Brute Force – Offline</td>
<td>• Digital Evidence</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 4.5.1 Digital Forensics Evidence</td>
<td>• Dictionary</td>
<td>Acquisition</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 4.5.2 Digital Forensics Evidence Acquisition</td>
<td>• Rainbow Table</td>
<td>• Steganography</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2.8.1 Hashing and Digital Signatures</td>
<td>• Steganography</td>
<td>• Biometrics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2.8.2 Elliptic Curves and Perfect Forward Secrecy</td>
<td>• File Hashing</td>
<td>• Equifax</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1.2.11 Password Attacks</td>
<td>• Collision</td>
<td>• MS-CHAP v2 Exploit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 4.1.7 Password Cracking Tools</td>
<td>• Cuckoo</td>
<td>• China’s Great</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2.8.3 Quantum Cryptography and Ephemeral Keys</td>
<td>• Obfuscation</td>
<td>Firewall</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2.8.4 Cryptography Modes of Operation and Blockchains</td>
<td>• Linux Personal File Encryption</td>
<td>• Heartbleed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2.8.5 Block Ciphers and Lightweight Cryptography</td>
<td>• Windows 7 Personal File Encryption</td>
<td>• Wireless Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2.8.6 Steganography and Homomorphic Encryption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2.8.7 Common Cryptography Use Cases</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2.8.8 Cryptography Limitations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actors and Vulnerabilities</td>
<td>1.1.1 Principles of Social Engineering</td>
<td>1.1.8 Credential Harvesting</td>
<td>1.1.2 Phishing and Spam</td>
<td>1.1.3 Dumpster Diving</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------------</td>
<td>---------------------------------------</td>
<td>-----------------------------</td>
<td>-------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Malware Attacks</td>
<td>Backdoor Shortcut</td>
<td>Botnet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.2.1 Malware</td>
<td>• Ransomware</td>
<td>• Malware</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.2.4 Viruses and Worms</td>
<td>• Backdoor</td>
<td>• Botnet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.2.2 Ransomware and Cryptomalware</td>
<td>• Intro to Keyloggers</td>
<td>• iPhone Integer Overflow</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.2.3 Trojans, Backdoors, and RATs</td>
<td>• Backdoor Removal</td>
<td>• Race Conditions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 4.1.6 Exploitation Frameworks</td>
<td>• Keylogger Application</td>
<td>• Chrome Crash Catastrophe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.2.9 Keyloggers</td>
<td>• Privilege Escalation</td>
<td>• Logic Bomb</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.3.1 Privilege Escalation</td>
<td>• Pass the Hash</td>
<td>• Wireless Disassociation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.3.7 Replay Attacks and Pass the Hash</td>
<td>• RAT/Bot</td>
<td>• Wireless Jamming</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.2.6 Bots and Botnets</td>
<td>• RAT Removal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.2.10 Rootkits</td>
<td>• Buffer Overflow</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.3.9 API and Resource Exhaustion Attacks</td>
<td>• Trojan</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.3.5 Buffer Overflows and Race Conditions</td>
<td>• Command Injection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.3.6 Error and Improper Input Handling</td>
<td>• SQL Injection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.2.5 PUPS and Fileless Viruses</td>
<td>• DVWA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.2.7 Logic Bombs</td>
<td>• Juice Shop Setup</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.2.8 Adware and Spyware</td>
<td>• fuzzing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.2.12 Physical Attacks</td>
<td>• Brute Force – Online</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.2.13 Adversarial AI</td>
<td>• XSS DVWA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.2.14 Supply-Chain Attacks</td>
<td>• XSS Juice Shop</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 4.1.6 Exploitation Frameworks</td>
<td>• Directory Traversal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.2.9 Keyloggers</td>
<td>• Intro to CSRF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.3.1 Privilege Escalation</td>
<td>• CSRF Application</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.3.7 Replay Attacks and Pass the Hash</td>
<td>• Session Replay</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.2.6 Bots and Botnets</td>
<td>• Honeypot</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.2.10 Rootkits</td>
<td>• MAC Spoofing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.3.9 API and Resource Exhaustion Attacks</td>
<td>• Denial of Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 1.3.5 Buffer Overflows and Race Conditions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organizational Security</td>
<td>2.1.1 Configuration Management</td>
<td>2.1.3 Security Concepts</td>
<td>2.2.1 Cloud Deployment Models</td>
<td>Certificates</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------</td>
<td>------------------------</td>
<td>-----------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>1.2.15 Cloud-Based vs On-Premises Attacks</td>
<td>1.3.10 Memory Leaks and SSL Stripping</td>
<td>1.3.11 Driver Manipulation Attacks</td>
<td>1.3.3 Data Injection</td>
</tr>
<tr>
<td>3.9.2 PKI Certificates</td>
<td>3.9.3 PKI Certificate Formats</td>
<td>3.9.4 PKI Concepts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------</td>
<td>---------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1.1 Security Controls</td>
<td>5.2.1 Security Regulations</td>
<td>5.2.2 Security Frameworks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.2.3 Security Guides</td>
<td>5.3.1 Personnel Management</td>
<td>5.3.2 Personnel Agreements and Policies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.4.1 Risk Types</td>
<td>5.4.2 Risk Management Strategies</td>
<td>5.4.3 Risk Assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.4.4 Business Impact Analysis</td>
<td>5.5.1 Organizational Breach Consequences</td>
<td>5.5.2 Handling Sensitive Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.5.3 Data Roles and Responsibilities</td>
<td>5.5.4 Data Assessments, Agreements, and Notices</td>
<td>(Cybersecurity, 2022)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix I: Cyber.org Cybersecurity Curriculum Artifacts

Syllabus Template

Syllabus for Cybersecurity
(CYBER.ORG Partnership)

About this course:
Cybersecurity lays a Foundation For understanding cyber law and policy, Linux, networking technology basics, risk assessment, cryptography, and a variety of cybersecurity tools - all the essential knowledge and skills needed to begin a Future in the cybersecurity workforce. Not only does Cybersecurity introduce the breadth of cybersecurity concepts and skills to students, but it also prepares them to verify their technical know-how through the CompTIA Security+ certification.

At the end of this course, you will:

- Understand the concepts behind cybersecurity (lessons)
- Practice a variety of cybersecurity skills in a safe setting (labs)
- Have a greater understanding of the history of cybersecurity (case studies)

Security+ Exam:
The content in the Cybersecurity course From CYBER.ORG is built around the CompTIA Security+ certification exam because it is an exceptional, industry-recognized certification. Additionally, it is a credential that has been approved by a variety of state departments of education as a contributing component to earning a diploma. The course introduces all the Security+ objectives SY0-601 as well as providing a secure and safe laboratory environment to practice those objectives. Students should be encouraged to obtain the certification before graduation, making them significantly more marketable as they pursue careers after high school.

Security+ Objectives:

- Threats, Attacks, and Vulnerabilities
- Architecture and Design
- Implementation
- Operations and Incident Response
- Governance, Risk, and Compliance
**Required Resources:**
Within this course, there are labs in the Form of hands-on exercises that demonstrate an attack, example, or tool that help support the lessons. An attack lab will demonstrate a real-world example of how a malicious user can attack an unsuspecting user's system and how this user can defend themselves. An example Lab has users run through a concept and see an example of how things work. The tool Lab explores different tools used in penetration and vulnerability testing. The Labs use a pair of Kali Linux and Windows 7 machines connected on the same network. The Labs are meant to run on the CYBER.ORG Range which is grant Funded. Teachers can request access to the no cost CYBER.ORG Range at https://apps.cyber.org.

**Instructional Units:**
1. Linux Basics (20 hours)
2. Security Basics (35 hours)
3. Actors and Vulnerabilities (30 hours)
4. Malware and Attacks (60 hours)
5. Organizational Security (35 hours)

**Sequencing:**
There are a total of 155 Lessons within the instructional units above. Every Lesson is a short instructional moment that is designed to introduce a concept and prepare for an exercise. It is the intent of the curriculum design team for teachers to present multiple Lessons in a 50- or 80-minute class and supplement them with a Lab or case study. While the numbered List provides a suggested order of delivery. For the content, it is only a recommendation. Classroom teachers may present Lessons in any order that works best for their classroom and students' needs. Pacing, scheduling differences, and student Learning differences will affect timelines differently.

Suggested contact hours are stated in parentheses.

**Student Diversity and Equity:**
CYBER.ORG believes in empowering all students. By expanding student participation in cybersecurity and computer science, we hope to enable student agency in a range of disciplines. Delving into a variety of topics, the course seeks to demystify the technological world around us and, in turn, provide opportunities for Further Learning through personal curiosity.

(Cybersecurity, 2022)
Cybersecurity

Hoaxes

(Cybersecurity, 2022)
Case Study - Cyber Laws

Article: Hacker ‘Coolio’ Pleads Guilty
JAN 02, 2001
Author: Associated Press

OSSIPEE, N.H.(AP) — A teen-age hacker who was briefly linked to a highly publicized series of hacking attacks against major companies pleaded guilty Tuesday to three misdemeanors. Dennis Moran, 18, who went by the name of “Coolio,” broke into rsa.com, operated by Internet security company RSA Security, and dare.com, an anti-drug site connected to the Los Angeles Police Department. If a judge approves a plea agreement, Moran will serve nine months to a year in jail and pay $5,000 in restitution to each of three victims.

Wearing a hooded sweatshirt and jeans, Moran said little during the half-hour hearing in Carroll County Superior Court and declined to talk to reporters afterward.

“I feel the disposition is fair for the crimes I committed,” he told Judge James O’Neill.

Prosecutor Michael Delaney disclosed that Moran also got onto the Web sites of four military bases, three Army, one Air Force. Getting onto the sites potentially gave him access to classified information, but he never actually accessed anything classified, Delaney said.

Moran, who lives with his father in Wolfeboro, will be formally sentenced this spring after a presentencing investigation. He pleaded guilty to unauthorized access to computer systems.

He will remain free on bail until his sentencing. He may use computers provided he does not do anything illegal with them.
The break-in onto the DARE site occurred at about the same time as publicized disruptions of major sites such as Yahoo! and eBay. Moran had allegedly bragged about those attacks but later said he had only been joking. A Canadian teen-ager who uses the computer name “mafiaboy” was later charged with disrupting eBay and Yahoo!

When he was first identified, Moran spoke freely to reporters. He was depicted as a polite, intelligent teen who dropped out of high school because he was bored and read Tolstoy after investigators confiscated the family’s computers. He soon changed his mind about interviewers and has remained silent since.

He went onto the DARE site twice a year ago, defacing it with pro-drug slogans and images, including one depicting Donald Duck with a hypodermic syringe in his arm.

The Web site of RSA — which proclaims itself “the most trusted name in e-security” — was linked to another hacked computer at a university in South America. There, a nearly duplicate hoax site proclaimed: “Trust us with your data! Praise Allah!”

The hacker left a message, “owned by coolio,” and derided RSA’s earlier announcement that it had developed a countermeasure to the types of attacks that had been launched against eBay.

Article:
Hacker Sentenced, Must Program Jail Computers

JAN 1992
Source: MIT.edu
Author: Brendan P. Kehoe

On November 2, 1988, Robert Morris, Jr., a graduate student in Computer Science at Cornell, wrote an experimental, self-replicating, self-propagating program called a worm and injected it into the Internet. He chose to release it from MIT, to disguise the fact that the worm came from Cornell. Morris soon discovered that the program was replicating and reinfecting machines at a much faster rate than he had anticipated—there was a bug. Ultimately, many machines at locations around the country either crashed or became “catatonic.” When Morris realized what was happening, he contacted a friend at Harvard to discuss a solution. Eventually, they sent an anonymous message from Harvard over the network, instructing programmers how to kill the worm and prevent reinfection. However, because the network route was clogged, this message did not get through until it was too late. Computers were affected at many sites, including universities, military sites, and medical research facilities. The estimated cost of dealing with the worm at each installation ranged from $200 to more than $53,000.

The program took advantage of a hole in the debug mode of the Unix sendmail program, which runs on a system and waits for other systems to connect to it and give it email, and a hole in the finger daemon fingerd, which serves finger requests. People at the University of California at Berkeley and MIT had copies of the program and were actively disassembling it (returning the program back into its source form) to try to figure out how it worked.
Teams of programmers worked non-stop to come up with at least a temporary fix, to prevent the continued spread of the worm. After about twelve hours, the team at Berkeley came up with steps that would help retard the spread of the virus. Another method was also discovered at Purdue and widely published. The information didn’t get out as quickly as it could have, however, since so many sites had completely disconnected themselves from the network.

After a few days, things slowly began to return to normalcy, and everyone wanted to know who had done it all. Morris was later named in The New York Times as the author (though this hadn’t yet been officially proven, there was a substantial body of evidence pointing to Morris).

Robert T. Morris was convicted of violating the computer Fraud and Abuse Act (Title 18), and sentenced to three years of probation, 400 hours of community service, a fine of $10,050, and the costs of his supervision. His appeal, filed in December 1990, was rejected the following March.

Summary
The first article talks about Dennis Moran, who defaced and altered multiple websites, including DARE’s, RSA Security’s, and some military bases’ websites when he was 17 years old. When he was 18, he was tried and convicted for 9-12 months in prison and to pay $5000 to three different victims.

The second article is about Robert Morris Jr., who created a worm while attending MIT. When testing the worm, it grew faster than he anticipated and became out of control. He attempted to stop the worm, but it affected universities, military sites, medical facilities, etc…; Morris received 3 years of probation, 400 hours of community service, and a $10,050 fine.

Questions
- Should someone under the age of 18 be able to serve prison time for a cyber-crime? Why or why not?
- Should teenagers be tried as adults and serve prison time even if they were 17 when they committed the crime? Why or why not?
- Was Moran’s punishment fair, or should it have been more or less harsh?
- Should Morris have been convicted for affecting systems he did not purposely infect? Why or why not?
- Morris’s worm caused more damage than Moran affected websites; should Morris have received pris- on time like Moran received? Why or why not?

Further Study
- Computer Fraud and Abuse Act 18: https://www.everycrsreport.com/reports/97-1025.html
- Kevin Mitnick’s (an infamous ‘hacker’) trial and results: https://law.jrank.org/pages/3791/Kevin-Mitnick-Case-1999.html
- Wired’s article on Robert Morris: https://www.wired.com/2011/07/0725first-computer-fraud-indictment/
- Wired’s article on Dennis Moran: https://www.wired.com/2001/01/coolio-pleads-guilty-to-hacking/

(Cybersecurity, 2022)
Attacks, Threats, and Vulnerabilities
1.1.10 Hoaxes

What are hoaxes and how can a malicious actor use them for social engineering attacks?

Overview
The student will compare and contrast different types of social engineering techniques.

Grade Level(s)
10, 11, 12

Cyber Connections
- Threats & Vulnerabilities
- Networks & Internet
- Hardware & Software

Teacher Notes:
CompTIA SY0-601 Security+ Objectives

Objective 1.1
- Compare and contrast different types of social engineering techniques.
- Hoax
**Hoaxes**

**Hoaxing Around**
The simple definition for a *hoax* is a deception either humorous or malicious. The majority of hoaxes are not real threats but can be portrayed as real.

**So What’s the Big Deal?**
Although most hoaxes are not real, they are still a waste of time and effort. These hoaxes are typically emails, such as a chain letter, depicting horrific events, urban legends, or malware. Some hoaxes can be an attempt to get money by phishing for login information. The attackers may pose as law enforcement or governmental agents. Their intent is to mislead and frighten victims, hoping to get the victims to forward the hoax to friends and family. For the hoaxes that pose no real danger, they may waste as much time and money as a real virus would.

**There Aren’t That Many, Right?**
There are over 100 documented hoaxes online (more if you consider innocent April Fool’s Day pranks). There’s a fine line between hoax and conspiracy so here’s a quick list of some well-known hoaxes:

- The disappearing blonde gene/redhead gene
- A stock manipulation scheme (Emulex is a classic case)
- The “gorgeous guy” (similar to what is used in catfishing)
- The Jackalope (sorry, it is not real)
- Crop circles (some may argue conspiracy on this one)
- The Mars hoax (claim that Mars will appear as large as the moon on a certain date)
- Planet X/Nibiru (typically claims that there is a rogue planet in our solar system that will eventually collide with the Earth)

**Defense**
As intimidating as it might sound, avoiding these hoaxes is relatively easy. Unless you were expecting an email with a provided link, do not click links in an email. For any link provided in an unknown email, go directly to the website claimed in the email, i.e. bank website, IRS website, etc. For the hoaxes with myths/urban legends, check credible sources like Snopes (for the most part, political claims are fact checked on Politifact, but some bias allows for a few inaccuracies). Finally, trust your spam filters. Recurring hoaxes are typically caught by major email providers like Google, Yahoo, and Outlook. And never blindly share or forward a hoax. Stay on alert and fact check, fact check, fact check.

(Cybersecurity, 2022)
1. Why might a person run a hoax?

2. Do all hoaxes have to have malicious intent?

3. Why might April 1st be a popular day for hoaxes?

4. How can a person defend themselves against a hoax?

5. What is a real-life example of a hoax that victims believed?

6. In the Hoax Case Study, what did the Tuxissa virus threaten to install on a person’s machine?

(Cybersecurity, 2022)
Quiz Example

1. What is a hoax?
   A. A humorous or malicious deception
   B. Higher Operational Auxiliary eXecutable
   C. A secret plan by a group to do something unlawful or harmful
   D. None of the above
   Answer: ________

2. Why are hoaxes considered a threat?
   A. They waste time and effort
   B. They seek login information
   C. They instill fear in their victims
   D. All of the above
   Answer: ________

3. Which of the following is NOT typically depicted in a hoax?
   A. Tragic events
   B. Malware/viruses
   C. Influenza
   D. Urban legends/myths
   Answer: ________

4. Which of the following is a confirmed hoax?
   A. The Liger
   B. The Jackalope
   C. The Wholphin
   D. The Beefalo
   Answer: ________

5. Which of the following is a confirmed hoax?
   A. Nibiru
   B. Crop circles
   C. The Moon landing is fake
   D. All of the above
   Answer: ________

6. Which of the following is a confirmed hoax?
   A. The blonde gene is disappearing
   B. Cheetahs can't roar
   C. If you (could) fold a piece of paper 42 times, it would reach the moon
   D. "umop apisdn" is "upside down" spelled upside down with different letter of the alphabet
   Answer: ________

(Cybersecurity, 2022)
Appendix J: Basha High School Cyber Program Profile

Enrollment

<table>
<thead>
<tr>
<th>Academic Year</th>
<th>Grade 9</th>
<th>Grade 10</th>
<th>Grade 11</th>
<th>Grade 12</th>
<th>Total</th>
<th>Graduates</th>
</tr>
</thead>
<tbody>
<tr>
<td>2022 – 2023</td>
<td>41</td>
<td>44</td>
<td>46</td>
<td>23</td>
<td>154</td>
<td>16</td>
</tr>
<tr>
<td>2021 – 2022</td>
<td>50</td>
<td>63</td>
<td>26</td>
<td>10</td>
<td>149</td>
<td>2</td>
</tr>
<tr>
<td>2020 – 2021</td>
<td>88</td>
<td>19</td>
<td>15</td>
<td>3</td>
<td>125</td>
<td>1</td>
</tr>
<tr>
<td>2019 – 2020</td>
<td>42</td>
<td>8</td>
<td>7</td>
<td>3</td>
<td>60</td>
<td>1</td>
</tr>
</tbody>
</table>

2022 – 2023 School Year

<table>
<thead>
<tr>
<th>Grade Level</th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
<th>Year 4</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>9th</td>
<td>41</td>
<td></td>
<td></td>
<td></td>
<td>41</td>
</tr>
<tr>
<td>10th</td>
<td>20</td>
<td>24</td>
<td></td>
<td></td>
<td>44</td>
</tr>
<tr>
<td>11th</td>
<td>11</td>
<td>5</td>
<td>26</td>
<td>4</td>
<td>46</td>
</tr>
<tr>
<td>12th</td>
<td>6</td>
<td>4</td>
<td>1</td>
<td>12</td>
<td>23</td>
</tr>
<tr>
<td>Total</td>
<td>78</td>
<td>33</td>
<td>27</td>
<td>16</td>
<td>154</td>
</tr>
</tbody>
</table>

* Year 3 Students are taking Year 3 and Year 4 courses.

2021 – 2022 School Year

<table>
<thead>
<tr>
<th>Grade Level</th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
<th>Year 4</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>9th</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td>50</td>
</tr>
<tr>
<td>10th</td>
<td>25</td>
<td>38</td>
<td></td>
<td></td>
<td>63</td>
</tr>
<tr>
<td>11th</td>
<td>11</td>
<td>3</td>
<td>12</td>
<td></td>
<td>26</td>
</tr>
<tr>
<td>12th</td>
<td>6</td>
<td>3</td>
<td>1</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>Total</td>
<td>92</td>
<td>44</td>
<td>13</td>
<td></td>
<td>149</td>
</tr>
</tbody>
</table>

2020 – 2021 School Year

<table>
<thead>
<tr>
<th>Grade Level</th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
<th>Year 4</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>9th</td>
<td>59</td>
<td>29</td>
<td></td>
<td></td>
<td>88</td>
</tr>
<tr>
<td>10th</td>
<td>18</td>
<td>1</td>
<td></td>
<td></td>
<td>19</td>
</tr>
<tr>
<td>11th</td>
<td>12</td>
<td>3</td>
<td></td>
<td></td>
<td>15</td>
</tr>
<tr>
<td>12th</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>91</td>
<td>34</td>
<td></td>
<td></td>
<td>125</td>
</tr>
</tbody>
</table>

2019 – 2020 School Year

<table>
<thead>
<tr>
<th>Grade Level</th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
<th>Year 4</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>9th</td>
<td>42</td>
<td></td>
<td></td>
<td></td>
<td>42</td>
</tr>
<tr>
<td>10th</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>11th</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>12th</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>60</td>
<td></td>
<td></td>
<td></td>
<td>60</td>
</tr>
</tbody>
</table>

Demographics

<table>
<thead>
<tr>
<th>Demographic</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>White</td>
<td>59.7%</td>
</tr>
<tr>
<td>Hispanic / Latino</td>
<td>13.6%</td>
</tr>
<tr>
<td>Asian or Asian / Pacific Islander</td>
<td>10.4%</td>
</tr>
<tr>
<td>Black or African American</td>
<td>11%</td>
</tr>
<tr>
<td>American Indian or Alaska Native</td>
<td>2%</td>
</tr>
<tr>
<td>Other or Undeclared</td>
<td>3.3%</td>
</tr>
</tbody>
</table>
Demographic Data represents the most recent data obtained for 2022 – 2023 school year.

Operations

Personnel

<table>
<thead>
<tr>
<th>Teacher</th>
<th>Education Level</th>
<th>Certifications</th>
<th>Years of Experience</th>
<th>Courses Taught</th>
<th>Dual Enrollment Qualified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Janet Hartkopf</td>
<td>MS Curriculum &amp; Instruction - Technology</td>
<td>CTE Certified</td>
<td>11 Years</td>
<td>Security Fundamentals, Ethics in IT</td>
<td>Y</td>
</tr>
<tr>
<td>Sam Alexander</td>
<td>BS Biology AS Cisco Networking</td>
<td>CTE Certified MTA Java</td>
<td>25 years</td>
<td>Hardware and Software Configurations, LAN &amp; Security Fundamentals</td>
<td>Y</td>
</tr>
<tr>
<td>Jyoti Tamboli</td>
<td>MS Computer Applications</td>
<td>CTE Certified STEM Certified</td>
<td>3 Years</td>
<td>CYB 120 - Introduction to Computer Systems, CSC 305 – Java – Computer Science, CSC 125 – AP Computer Science Principles, CYB 300 – Linux Administration (RHEL)</td>
<td>Y</td>
</tr>
</tbody>
</table>

Equipment

<table>
<thead>
<tr>
<th>Equipment Type</th>
<th>Make</th>
<th>Model</th>
<th>Quantity</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Kit</td>
<td>Basha HS Equipment List</td>
<td>31</td>
<td>$25,000</td>
<td></td>
</tr>
<tr>
<td>Misc. Tools</td>
<td>Basha HS Lab Tool List</td>
<td>N/A</td>
<td>$2,346.97</td>
<td></td>
</tr>
<tr>
<td>Locking Storage</td>
<td>ULINE</td>
<td>H-6839</td>
<td>1</td>
<td>$1,300</td>
</tr>
<tr>
<td>Networking</td>
<td>Cisco</td>
<td>CCNA 200-301</td>
<td>4</td>
<td>$3,638.84</td>
</tr>
<tr>
<td>PCs &amp; Monitors</td>
<td>“Chromebook” type laptop with ability to use PacketTracer</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Network

- Chandler Unified School District provided network access.
  - Isolated network provided for cybersecurity classrooms and lab spaces.
    - Requires separate hardware and non-district issued machines.
    - Allows access websites, resources, and facilitates meeting the learning objectives of courses.

Facilities

- School has dedicated classroom space for cybersecurity program.
  - Three general purpose classrooms and one Career and Technical Education (CTE) Lab.
- CTE lab space provides larger footprint. Consists of teaching space and space for hands on activities and equipment storage.
- Classrooms have webcams and in-classroom microphones (2) to support video-conferencing capabilities.

### Formal Learning Activities

<table>
<thead>
<tr>
<th>Course</th>
<th>Company</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYB 240A / CNT 140 – Intro to LAN &amp; Security Fundamentals</td>
<td>Cisco</td>
<td>* Free Courseware</td>
</tr>
<tr>
<td>CYB 240B / CNT 150 – Intro to LAN &amp; Security Fundamentals</td>
<td>Cisco</td>
<td>* Free Courseware</td>
</tr>
<tr>
<td>CYB 300A / CIS 126DL – Linux OS</td>
<td>Cisco</td>
<td>$30 per student lab fee</td>
</tr>
<tr>
<td>CYB 300B / CIS 238DL – Advanced Linux Fundamentals</td>
<td>Cisco</td>
<td>$30 per student lab fee</td>
</tr>
<tr>
<td>CYB 400A / CIS 110 – Information Security Fundamentals</td>
<td>TestOut</td>
<td>$2,900 per year (50 user license)</td>
</tr>
<tr>
<td>CYB 400B / CIS 111 – Ethics in Information Technology</td>
<td>Cengage</td>
<td>$4,620 for Print Student Edition + 6 years access to online platform MindTap x 40 (price includes shipping and processing)</td>
</tr>
<tr>
<td>CYB 130 / CIS 156 – Python</td>
<td>Cisco</td>
<td>* Free Courseware</td>
</tr>
</tbody>
</table>

* Must be member of Western Academy Support & Training Center – WATSC (~$500 per year)

- Reverse engineered from Chandler Gilbert Community College (CGCC) four year plan to ensure articulation and pathway for students.
- Completing fourth year of the program in School Year 2022 – 2023.
- Program used RedHat Linux content through 2022 – 2023 School Year. Will switch to Cisco content after 2022 – 2023 school year.

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Syllabus</th>
<th>Dual Enrollment</th>
<th>Pre-Existing</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYB 120 / CIS 105 – Introduction to Computer Systems</td>
<td>Overview of computer technology, concepts, terminology, and the role of computers in business and society. Discussion of social and ethical issues related to computers. Use of word processing, spreadsheet, database, and presentation software. Includes uses of application software and the Internet for efficient and effective problem solving. Exploration of relevant emerging technologies.</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>CYB 230 A / BPC 170 – Hardware and Software Config &amp; Support</td>
<td>This course provides an excellent introduction to the IT industry and interactive exposure to personal computers, hardware, and operating systems. Students participate in hands-on activities and lab-based learning to become familiar with various hardware and software components and discover best practices in maintenance and safety.</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>CYB 230 B / BPC 270 – Hardware and</td>
<td>This course provides an excellent introduction to the IT industry and interactive exposure to personal computers, hardware, and operating systems.</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>
**Software Config & Support**

Systems. Students participate in hands-on activities and lab-based learning to become familiar with various hardware and software components and discover best practices in maintenance and safety.

**CYB 240 A / CNT 140 – Intro to LAN & Security Fundamentals**

This course teaches the fundamentals of networking. It covers how devices communicate on a network, network addressing and network services, how to build a home network and configure basic security, the basics of configuring Cisco devices, and testing and troubleshooting network problems.

| | Y | Y | N |

**CYB 240 B / CNT 150 – Intro to LAN & Security Fundamentals**

This course teaches the fundamentals of networking. It covers how devices communicate on a network, network addressing and network services, how to build a home network and configure basic security, the basics of configuring Cisco devices, and testing and troubleshooting network problems.

| | Y | Y | N |

**CYB 300 A / CIS 126DL – Linux OS**

Introduction to the Linux Operating system. Develop knowledge and skills required to install, configure, and troubleshoot a Linux-based workstation including basic network functions. Learn basic command line and Graphical User Interface (GUI) desktop environment utilities and applications. Fundamental abilities to achieve the entry-level industry certification covered.

| | Y | Y | N |

**CYB 300 B / CIS 238DL – Advanced Linux**

Managing Linux Operating Systems including sophisticated manipulation of file structures, backup systems, printing processes, troubleshooting, user account management, hard disk maintenance and configuration, process monitoring and prioritizing, kernel customization, and system resource control. Preparation for industry certifications such as the CompTIA Linux+, the Red Hat Certified System Administrator (RHCSA), the Red Hat Certified Engineer (RHCE) and the Linux Professional Institute (LPIC-1).

| | Y | Y | N |

**CYB 400A / CIS 110 – Information Security Fundamentals**

Fundamental concepts of information technology security. Topics include authentication methods, access control, cryptography, Public Key Infrastructure (PKI), network attack and defense methods, hardening of operating systems and network devices, securing remote access and wireless technologies, and securing infrastructures and topologies. Emphasis on hands-on labs in both the Windows and Linux environments. Builds on thorough understanding of TCP/IP and security concepts and Microsoft (MS) Windows and Linux Administration.

| | Y | Y | N |

**CYB 400B / CIS 111 – Ethics in**

Ethical issues that arise as a result of increasing use of computers, and the responsibilities of those who work with computers, either as

| | Y | Y | N |
### Information Technology

Critical inquiry and review of ethical challenges in information technology business, including professional and corporate responsibility, government regulation, fiduciary responsibilities of information, infringement of intellectual property, security risk assessment, Internet crime, identity theft, employee surveillance, privacy, compliance, social networking, and the ethics of IT corporations.

### CYB 130 / CIS 156 - Python

Introduction to Python programming. Includes general concepts, program design, development, data types, operators, expressions, flow control, functions, classes, input, and output operations, debugging, structured programming, and object-oriented programming.

<table>
<thead>
<tr>
<th></th>
<th>Y</th>
<th>Y</th>
<th>N</th>
</tr>
</thead>
</table>

### Non-Formal Learning Activities

#### Camps
- AZ Cyber Initiative
- CyberPatriot

#### Certifications
- A+
- ITF+
- Linux+
- Security Pro
- Security+
- Python PCEP

#### Internships
- Open Source Integrators

#### Externships
- ElevateEd AZ
- Cybersecurity and Technology Externship

### Informal Learning Activities

#### Clubs
- Future Business Leaders of America (FBLA)

#### Competitions
- National Cyber League
- CyberPatriot

#### Self-Study / Ad-Hoc Learning
Students are provided a variety of resources for additional learning outside of the classroom. Examples include cyber.org range access, Professor Messer videos, YouTube videos, and other resources.

#### Conferences
- CactusCon
- WiCYS
- K12 NICE Conference – Student Signing Day
- Embry Riddle Aeronautical Engineering Cyber Day

#### Industry Events
- PhoenixNap Tour

### Pathways

#### Post-Secondary
- Chandler Gilbert Community College (CGCC) Cybersecurity AAS

#### Trade or Certification Program
- Advanced Business Learning (ABL)

#### Military
- Air Force JROTC

#### Workforce
- Kelly Technologies
Survey of Computer Information Systems

Course: CIS105
Course Type: Occupational
Loc + Lab 3.0 Credit(s) 4.0 Period(s) 4.0 Load
Load Formula: T
First Term: 2018 Fall
Final Term: Current

Description: Overview of computer technology, concepts, terminology, and the role of computers in business and society. Discussion of social and ethical issues related to computers. Use of word processing, spreadsheet, database, and presentation software. Includes uses of application software and the Internet for efficient and effective problem solving. Exploration of relevant emerging technologies.

Requisites: None.

Course Attributes:
General Education Designation: Computer/Statistics/Quantitative Applications - [CS]
Arizona Shared Unique Number SUN#: CIS 1120

MCCCD Official Course Competencies
1. Identify common hardware components of computer systems and describe their uses. (I)
2. Identify different types of software and their uses. (II)
3. Describe common uses of networks. (III)
4. Describe Website Technology. (IV)
5. Use the Internet to communicate, collaborate, and retrieve information. (IV, VII)
6. Explore system security and privacy issues. (III, IV, VII)
7. Create macros and understand the basics of Visual Basic for Applications (VBA). (V)
8. Describe the steps in planning and implementing technology solutions. (VI)
9. Determine when technology is useful and select the appropriate tool(s) and technology resources to address a variety of tasks and problems. (VI, VIII)
10. Identify terminology and the uses of technology in business and society, including limitations. (VI)
11. Identify positive social and ethical behaviors when using technology and the consequences of misuse. (VII)
12. Describe how technology is used in the departments of a business and in various career paths. (VIII)
13. Use word processing, spreadsheet, database, and presentation software. (IX)

MCCCD Official Course Outline

I. Hardware
   A. Processing Unit
   B. Storage Devices
   C. Input Devices
   D. Output Devices
   E. Network Technology
   F. Internet Technology

https://arizona.maricopa.edu/csv-em/WeblObjects/MCCCD.wbin/wafreeForm2?id=128924
I. Software
   A. System Software
      1. Operating System
      2. Utilities
      3. Device Drivers
   B. Application Software
      1. Word Processing
      2. Spreadsheets
      3. Databases
      4. Presentation Software
   C. Specialized Application Software
   D. Web Authoring Application Software

II. Networks
   A. Types of Networks
      1. Local Area Network (LAN)
      2. Wide Area Network (WAN)
   B. Uses of Networks
      1. Sharing Resources
      2. Communication
   C. Security and Data Integrity

IV. Internet
   A. History
   B. World Wide Web Structure
   C. Browsers
   D. Search Engines
   E. E-mail
   F. e-Commerce
   G. Hypertext Markup Language (HTML)
   H. Security
   I. Intranet
   J. Websites

V. Visual Basic Application (VBA)
   A. Visual Basic Editor
      1. Procedures
      2. Variables
   B. Macros
      1. Excel
      2. Access

VI. Planning and Implementing Technology Solutions
   A. Information Systems Role in Business
   B. Purchasing and Upgrading Microcomputers

VII. Social and Ethical Issues
   A. Ethics
   B. Viruses
   C. Security
   D. Ergonomics
   E. Intellectual Property Rights
   F. Privacy
   G. Green Computing

VIII. Uses of Technology
   A. Business
IX. Business Application Tools
A. Word
1. Editing and formatting
2. Creating and modifying
   a. Styles
   b. Table of Contents
   c. Index
B. PowerPoint
1. Create and modify
   a. Slideshows
   b. Templates
   c. Outlines
C. Excel
1. Create, edit, and format spreadsheets
2. Create and modify formulas
3. Use Excel functions
4. Create and modify charts
5. Table Management
   a. Sort
   b. Filter
   c. Import data
   d. Database functions
   e. Create, refresh, and delete
      (1) Pivot tables
      (2) Pivot charts
D. Access
1. File management
   a. Design data
   b. Create tables
2. Manage data
   a. Filter
   b. Sort
   c. Query
   d. Report
   e. Pivot table
      (1) View
      (2) Chart
   f. Structured Query Language (SQL)

MCCCD Governing Board Approval Date: 5/25/2010

All information published is subject to change without notice. Every effort has been made to ensure the accuracy of information presented, but based on the dynamic nature of the curriculum process, course and program information is subject to change in order to reflect the most current information available.
**Course: BPC170**  
**Lec + Lab 3.0 Credit(s)**  
**4.0 Period(s)**  
**4.0 Load**  
**Course Type: Occupational**  
**First Term: 2020 Fall**  
**Final Term: Current**

**Description:** Explore technical aspects of personal computers, including system components, installation, system configuration, peripheral devices, and notebooks. Emphasis placed on hardware installation, maintenance, mobile devices, and hardware troubleshooting. Helps prepare students for the CompTIA A+ examinations.

**Requisites:** Prerequisites: None.

**MCCCD Official Course Competencies**

1. Identify the fundamental principles of using personal computers. (I, II, III)
2. Identify, install, configure, optimize, and upgrade personal computer components using appropriate tools. (I, II, III)
3. Identify the fundamental principles of networks. (IV)
4. Identify and describe network hardware and network media and their uses in given scenarios. (IV)
5. Install, configure, and deploy wired and wireless networks using appropriate tools and network components based upon given scenarios. (IV)
6. Identify the fundamental principles of using laptops. (V)
7. Install, configure, optimize, and upgrade laptops using appropriate tools. (V)
8. Identify the fundamental principles of using printers. (VI)
9. Install, configure, maintain, and share printers based upon given scenarios. (VI)
10. Explain the theory, processes, and best practices for troubleshooting hardware components, peripherals, mobile devices, and networking. (VII)
11. Identify symptoms and use the tools needed to fix hardware components, peripherals, mobile devices, and networking based upon given scenarios. (VII)

**MCCCD Official Course Outline**

I. Personal computers and components  
   A. Connection interfaces and their purposes  
      1. Serial, parallel, PS/2  
      2. Universal Serial Bus (USB)  
      3. IEEE 1394  
   B. Components  
      1. Cases  
      2. Motherboards  
      3. Processors  
      4. Memory  
      5. Expansion cards  

https://aztransmac2.asu.edu/cgi-bin/WebObjects/MCCCD.wca/wa/freeForm2?id=153893
6. Power supplies
7. Cooling
C. Basic Input/Output System (BIOS) settings and security

II. Peripheral devices
A. Device connector types and associated cables
B. Display devices
   1. Analog
   2. Digital
   3. Multiple displays
C. Install drivers
D. Modify settings and properties

III. Storage
A. Storage devices
   1. Floppy disk
   2. Hard disk
   3. Optical discs
   4. Flash devices
   5. Solid state drives
   6. Tape drives
B. Connection types and associated cables
   1. Parallel ATA (PATA)
   2. Serial ATA (SATA)
   3. Small Computer System Interface (SCSI)
   4. USB/Firewire
   5. Ethernet
C. Redundant Array of Independent Discs (RAID)

IV. Networking
A. Network types
   1. Local Area Network (LAN)
   2. Wide Area Network (WAN)
   3. Personal Area Network (PAN)
   4. Metropolitan Area Network (MAN)
   5. Topologies
B. Network devices
   1. Network adapter
   2. Hub
   3. Switch
   4. Router
   5. Bridge
C. Network cables and connectors
   1. Coaxial
   2. Twisted pair
   3. Fiber optic
D. Network addressing
   1. Mac addresses
   2. Logical addresses
   3. Internet Protocol (IP) class
      a. Class A
      b. Class B
      c. Class C
   4. Static vs. dynamic
5. Client-Side Domain Name System (DNS)
6. Dynamic Host Configuration Protocol (DHCP)
7. Subnet mask
8. Gateway
E. Transmission Control Protocol (TCP) vs. User Datagram Protocol (UDP)
F. Common ports and protocols
G. Wireless networking
   1. IEEE standards
   2. Authentication
   3. Security and encryption
H. Small Office/Home Office Network (SOHO)
V. Laptop devices
   A. Hardware components and expansion options
   B. Power saving options
   C. Special function keys
   D. Display technology
      1. Liquid-Crystal Display (LCD)
      2. Light-Emitting Diode (LED)
      3. Organic Light-Emitting Diode (OLED)
      4. Plasma
VI. Printing
   A. Printer types
      1. Ink jet (ink dispersion)
      2. Laser
      3. Thermal
      4. Impact
   B. Imaging processes
      1. Electrophotographic (EP) process
      2. Hewlett-Packard (HP) process
      3. LED process
   C. Sharing
   D. Printer maintenance
VII. Hardware and network troubleshooting
   A. Troubleshooting theory and methods
   B. Hardware components
   C. Video
   D. Peripheral devices
   E. Networking

MCCCD Governing Board Approval Date: June 23, 2020

All information published is subject to change without notice. Every effort has been made to ensure the accuracy of information presented, but based on the dynamic nature of the curricular process, course and program information is subject to change in order to reflect the most current information available.
A+ Exam Prep: Operating System Configuration and Support

Course: BPC270  Lec + Lab  3.0 Credit(s)  4.0 Period(s)  4.0 Load
Course Type: Occupational
First Term: 2018 Fall  Load Formula: T
Final Term: Current

Description: Explore advanced technical aspects of maintaining and servicing computers. Emphasis placed on OS installation, maintenance, mobile devices, security, software troubleshooting, and on proper usage of tools, safety procedures, and professionalism. Helps prepare students for the CompTIA A+ examinations.

Requisites: Prerequisites: A grade of C or better in CIS105 or permission of Instructor.

MCCCD Official Course Competencies

1. Identify the fundamentals of using operating systems. (I)
2. Install, configure, optimize, upgrade, and perform preventive maintenance on operating systems using appropriate tools, diagnostic procedures, and troubleshooting techniques. (I, II, VIII)
3. Explain the purposes, requirements, and security measurements needed for implementing virtualization. (III)
4. Define the different types of disk storage and file systems and perform common disk management and file management procedures. (IV, V)
5. Utilize common techniques for managing folders and files, including setting permissions, file attributes, sharing between users. (V)
6. Identify the fundamental principles of security. (VI)
7. Implement security policy and procedure on wired and wireless networks based upon given scenarios, including selection of appropriate security components. (VI)
8. Install, configure, upgrade, optimize and perform preventive maintenance with respect to security using appropriate tools, diagnostic procedures, and troubleshooting techniques. (VI)
9. Compare the differences between mobile devices, including hardware, mobile operating systems, and security. (VII)
10. Describe communication methods for mobile devices. (VII)
11. Setup, configure, and use applications to retrieve and synchronize data between a mobile device and computer/server. (VII)
12. Explain the processes and best practices for troubleshooting and fixing problems with operating systems and applications. (VIII)
13. Identify symptoms and use the tools needed to fix problems with operating systems and applications. (VIII)
14. Use job-related professional behavior including communication skills, tact, notation of privacy, confidentiality, and respect for the customer and customer’s property. (IX)
15. Explain safe lab procedures and tool use. (IX)
16. Describe potential safety hazards and safety procedures associated with a variety of computer equipment. (IX)
17. Describe the aspects and importance of safety and environmental issues including potential hazards and proper safety procedures with respect to computer maintenance. (IX)
I. Operating System (OS)
   A. Parts of an Operating System
      1. Kernel
      2. Drivers
      3. Interface
      4. Utilities
      5. Applications
   B. Components of Windows
      1. Desktop
      2. Taskbar
      3. Notification Area
      4. Windows Explorer
      5. Control Panel
      6. User Account Control (UAC)
      7. HomeGroup
   C. Components of Mac
      1. Desktop
      2. KeyChain
      3. Finder
      4. Dock
      5. Boot Camp
   D. Components of Linux
      1. Desktop
      2. Linux Commands
   E. System Tools
   F. Preferences and Settings
      1. Users
      2. Virtual Memory
   G. Maintenance
      1. Performance Monitoring
      2. Install and Uninstall Applications
      3. Apply System and Application Updates
      4. System Protection

II. System Implementation
   A. Processes and Procedures for Pre-Installation of the OS
   B. Installing of the OS
   C. Processes and Procedures for Post-Installation of the OS

III. Virtualization
   A. Components Included in Virtualization
      1. Physical Machine
      2. Hypervisor
      3. Virtual Machine
      4. Virtual Hard Disk (VHD)
   B. Types of Virtualization
      1. Full
      2. Partial
      3. Paravirtualization
   C. Security Benefits and Issues

IV. Disk Management
   A. Disk Types
      1. Dynamic vs. Basic
      2. Primary
4. Primary
3. Extended
4. Logical
B. Disk Management
1. Drive Status
2. Adding Drives and Arrays
3. Mounting, Extending, and Splitting
C. Optimization and Maintenance
1. Disk Cleanup
2. Check Disk
3. Defrag
V. File Management
A. File System Components
1. Partition
2. Volume
3. Directory
4. File
B. File System Types
1. FAT/FAT32
2. New Technology File System (NTFS)
3. Compact Disc File System (CDFS)
C. Folder and File Management
1. Common File Locations for Windows
2. Common File Management Commands
D. Sharing Folders and Files
1. NTFS vs. Share Permissions
2. File Attributes
3. Cloud
VI. System Security
A. Attack and Intrusion Methods and Countermeasures
1. Social Engineering
2. Malware
B. Security Best Practices
1. Principle of Least Privilege
2. Account Management and Authentication
3. Encryption
C. Physical Security
1. Building Security
2. User Education
3. Data Destruction
D. Network Security
1. Network Utilities
2. Wired and Wireless Networks
3. Firewalls
4. Proxy Servers
VII. Mobile Devices
A. Laptop vs. Mobile Device Features
B. Operating Systems
C. Network Connectivity
D. System and Application Configuration
E. Securing
VIII. Software Troubleshooting
A. Operating System
B. Windows Recovery
C. System Errors
D. Security
E. Applications
F. Tools
G. Mobile Device
IX. PC Technician Role
   A. Job-Related Professional Behavior
      1. Communication and Professionalism
      2. Private and Confidential Materials
      3. Customer Focus
   B. Appropriate Tools to Ensure Safety
   C. Computer Evidence Collection and Analysis
   D. Appropriate Safety Procedures to Avoid Potential Hazards
      1. Electro-Static Discharge Precautions and Procedures
      2. Safe Work Environments
   E. Disposal Procedures for Equipment and Hazardous Chemicals

MCCCD Governing Board Approval Date: December 13, 2016

All information published is subject to change without notice. Every effort has been made to ensure the accuracy of information presented, but based on the dynamic nature of the curricular process, course and program information is subject to change in order to reflect the most current information available.
Cisco Networking Basics

Course: CNT140  Lec + Lab  4 Credit(s)  6 Period(s)  5.4 Load  
Course Type: Occupational  
First Term: 2007 Fall  Load Formula: S  
Final Term: 2017 Fall

Description: Introduction to the computer networking field. Covers network terminology and protocols, local area networks (LAN), and wide area networks (WAN). Includes Open Systems Interconnection (OSI) models, cabling and cabling tools, routers, router programming, Ethernet, Internet Protocol (IP) addressing, and network standards. Preparation for the Cisco Certified Network Associate examination.

Requisites: None

MCCCD Official Course Competencies
1. Explain physical connections of the computer to the Internet, connection testing, use of web browsers, and binary and hexadecimal numbers. (I)
2. Explain internetworking problems and solutions and their relationship to the seven layers of the Open Systems Interconnection (OSI) and the Transmission Control Protocol/Internet Protocol (TCP/IP) model. (II)
3. Describe the characteristics and types of cables and cabling specifications related to those devices. (III, IV)
4. Identify and describe the protocols, hardware, and cabling types related to local area networks (LANs) and wide area networks (WANs). (V)
5. Identify and describe Ethernet technology (VI, VII)
6. Identify and describe hardware devices used to work with broadcast and collision domains. (VI)
7. Explain concepts of binary and hexadecimal numbers and their conversion to and from decimal numbers. (VII)
8. Describe and demonstrate IP addressing and subnet masking, and explain how to obtain an Internet Protocol (IP) address. (VII, IX)
9. Contrast routed and routing protocols, and explain how subnetting relates to these practices. (VIII)
10. Describe and identify the protocols and technologies working at the Transport and Application layers of the Transmission Control/Internet Protocol TCP/IP model. (IX)

MCCCD Official Course Outline
I. Introduction to Networking
   A. Connecting to the Internet
   B. Network math
II. Networking Fundamentals
   A. Terminology
   B. Bandwidth
   C. Networking models
III. Networking Media

https://aztransmac2.asu.edu/cgi-bin/WebObjects/MCCCD.woa/va/freeForm2?id=50201
A. Copper media  
B. Optical media  
C. Wireless media  

IV. Cable Testing  
A. Frequency-based cable testing  
B. Signals and noise  
C. Methods of testing fiber optic cable  
D. Attenuation and signal loss  

V. Cabling LANS and WANS  
A. Cabling the LAN  
B. Cabling the WAN  
C. Serial, integrated services digital network (ISDN) and digital subscriber lines (DSL) interfaces on routers  

VI. Ethernet Fundamentals  
A. Basic principles  
B. Ethernet operation  
C. 10-Mbps and 100-Mbps Ethernet  
D. Gigabit and 10-Gigabit Ethernet  
E. Ethernet switching  
F. Collision and broadcast domains  

VII. TCP/IP Protocol Suite and IP Addressing  
A. Introduction to TCP/IP  
B. Internet addresses  
C. Obtaining an IP address  

VIII. Routing Fundamentals and Subnets  
A. Introduction to routers  
B. Routed vs routing protocols  
C. IP packet structure  
D. Route tables and path determination  
E. IP address classes and subnetting  

IX. TCP/IP Transport and Application Layers  
A. TCP/IP transport layer  
B. Three-way handshake and windowing flow control  
C. TCP vs user datagram protocol (UDP)  
D. The application layer and its protocols  
G. Cable installation  

VI. Cisco Troubleshooting Procedures  
A. Initial and subsequent testing  
1. Effects of EMI/RFI  
2. Causes of cross talk  
B. Safe wiring systems  
C. Solution strategies  

MCCCD Governing Board Approval Date: 6/26/2007  

All information published is subject to change without notice. Every effort has been made to ensure the accuracy of information presented, but based on the dynamic nature of the curricular process, course and program information is subject to change in order to reflect the most current information available.
Cisco - Routing and Switching Essentials

Course: CNT150AA  Lec + Lab  4.0 Credit(s)  6.0 Period(s)  6.0 Load
First Term: 2018 Fall  Course Type: Occupational
Final Term: Current  Load Formula: T

Description: Architecture, components, and operations of routers and switches in a small network. Students learn how to configure a router and a switch for basic functionality. Configuration and troubleshooting routers and switches and resolving common issues with RIPv1, RIPng, single-area and multi-area OSPF, virtual LANs, and inter-VLAN routing in both IPv4 and IPv6 networks. Preparation for Cisco certification examination.

Requisites: Prerequisites: A grade of C or better in CNT140AA or permission of Instructor.

MCCCD Official Course Competencies

1. Describe basic switching concepts and the operation of Cisco switches (I, II)
2. Describe the purpose, nature, and operations of a router, routing tables, and the route lookup process (IV, V, VI, VII)
3. Describe how VLANs create logically separate networks and how routing occurs between them (III, V)
4. Describe dynamic routing protocols, distance vector routing protocols, and link-state routing protocols (VII, VIII)
5. Configure and troubleshoot static routing and default routing (RIP and RIPng) (VI)
6. Configure and troubleshoot an Open Shortest Path First (OSPF) network (VIII)
7. Configure and troubleshoot access control lists (ACLs) for IPv4 and IPv6 networks (IX)
8. Configure and troubleshoot Dynamic Host Configuration Protocol (DHCP) for IPv4 and IPv6 networks (X)
9. Configure and troubleshoot Network Address Translation (NAT) operations (XI)

MCCCD Official Course Outline

I. Introduction to Switched Networks
   A. LAN Design
   B. The Switched Environment
II. Basic Switching Concepts and Configuration
   A. Basic Switch Configuration
   B. Switch Security: Management and Implementation
III. VLANs
   A. VLAN Segmentation
   B. VLAN Implementations
   C. VLAN Security and Design
IV. Routing Concepts
   A. Initial Configuration of a Router
   B. Routing Decisions
   C. Router Operation
V. Inter-VLAN Routing
   A. Inter-VLAN Routing Configuration
   B. Troubleshoot Inter-VLAN Routing
   C. Inter-VLAN Switching
C. Layer 3 Switching

VI. Static Routing
   A. Static Routing Implementation
   B. Configure Static and Default Routes
   C. Review of CIDR and VLSM
   D. Configure Summary and Floating Static Routes
   E. Troubleshoot Static and Default Route Issues

VII. Routing Dynamically
   A. Dynamic Routing Protocols
   B. Distance Vector Routing Protocols
   C. RIP and RIPng Routing
   D. Link-State Dynamic Routing
   E. The Routing Table

VIII. Single-Area OSPF
   A. Characteristics of OSPF
   B. Configuring Single-Area OSPFv2
   C. Configuring Single-Area OSPFv3

IX. Access Control Lists
   A. IP ACL Operation
   B. Standard IPv4 ACLs
   C. Extended IPv4 ACLs
   D. Troubleshoot ACLs
   E. IPv6 ACLs

X. DHCP
   A. Dynamic Host Configuration Protocol v4
   B. Dynamic Host Configuration Protocol v6

XI. Network Address Translation for IPv4
   A. NAT Operation
   B. Configuring NAT
   C. Troubleshooting NAT

MCCCD Governing Board Approval Date: June 24, 2014

All information published is subject to change without notice. Every effort has been made to ensure the accuracy of information presented, but based on the dynamic nature of the curricular process, course and program information is subject to change in order to reflect the most current information available.
Linux Operating System

Course: CIS 126DL
Lec + Lab 3.0 Credit(s) 4.0 Period(s) 4.0 Load
Course Type: Occupational

First Term: 2018 Fall
Final Term: Current

Description: Introduction to the Linux Operating system. Develop knowledge and skills required to install, configure and troubleshoot a Linux-based workstation including basic network functions. Learn basic command line and Graphical User Interface (GUI) desktop environment utilities and applications. Fundamental abilities to achieve the entry-level industry certification covered.

Requisites: None

MCCCD Official Course Competencies

1. Understand the history and nature of Open Source software (I)
2. Demonstrate ability to install a variety of Linux distributions. (II)
3. Compare and contrast variety of Linux distributions (II)
4. Navigate the Linux file system hierarchy (II)
5. Create, manage, and delete user accounts, groups and permissions. (II)
6. Demonstrate basic Linux shell commands including file and directory commands, archiving and compression. (III)
7. Use the Visual Editor (VI) to edit and create text documents. (III)
8. Configure printers for use on a workstation or network. (IV)
9. Understand X Window system architecture. (IV)
10. Use graphic utility to configure graphic display. (IV)
11. Research shell commands using the /etcshadow option and Manual (Man) pages. (V)
12. Install applications using Red Hat Package Manager (RPMs) and compression utilities such as Tape Archive (tar) and gzip. (V)
13. Use network-based applications such as browsers, telnet, file transfer protocol (FTP) and email. (V)
14. Demonstrate knowledge of a variety of GNU Object Model Environment (GNOME) and K Desktop Environment (KDE) applications. (V)
15. Troubleshoot problems related to operating system installation and configuration. (VI)

MCCCD Official Course Outline

I. Theory of Operation
   A. History of Open Source and Free Software
   B. How the Free Software Foundation’s (FSF) GNU (GNU’s Not Unix) Project lead to the General Public License (GPL)
   C. Third Party Analysis of Open Source Software
   D. Living with Free Software
   E. Linux System Concepts

https://www.maricopa.edu/.../WebObjects/MCCCD.xoo/webForm?id=125959
F. Main Board Configuration Issues
G. Network Configuration

II. Base System
A. Installation Media
B. Component Compatibility and Configuration Responsibilities
C. Describe several Linux distributions and their tradeoffs
D. Installation of Linux
E. Compare and Contrast several Different Distributions of Linux
F. Start Up and Shut Down Sequences
G. File System Hierarchy
H. Basic System Navigation
I. Manage User Accounts

III. Shells and Commands
A. The Shell
B. Single character commands (interrupt, erase, etc.)
C. The ls command - directory listing
D. The cd command - change directory
E. More and less commands - pager utilities
F. The cp command - copy a file
G. The ln command - duplicate a directory or filename
H. The mv command - move or rename a file
I. The mkdir command - make a directory
J. The rm command - remove a file
K. The rmdir command - remove a directory
L. The head and tail commands - peak at beginning or end of a file
M. The file command - view the file type
N. The grep command - search files for a target string
O. The du and df commands - show disk usage and free space
P. The tar command - places multiple files into one archive
Q. The gzip, gunzip, and zcat - un/compression utilities
R. The mtools - read and write MS-DOS files quickly
S. The find and locate - search for names in the file system
T. The Visual Editor (Vi) text editor

IV. System Services
A. Device Driver Utilities
B. Printer Configuration
C. The X Window System Architecture
D. Window Managers

V. Applications
A. Gathering Information
B. Network Applications including browser, email, telnet, secure shell, and file transfer
C. Text, Mark-up and Word Processing Programs
D. Office Applications
F. Graphics Applications

VI. Installation Troubleshooting
A. Linux Loader (LILO) and boot problems
B. Creation of rescue disks
C. Locked applications and processes
D. Printing errors
E. System logging
MCCCD Governing Board Approval Date: 12/9/2003

All information published is subject to change without notice. Every effort has been made to ensure the accuracy of information presented, but based on the dynamic nature of the curricular process, course and program information is subject to change in order to reflect the most current information available.
Linux System Administration

Course: CIS238DL  
Lec + Lab 3.0 Credit(s) 4.0 Period(s) 4.0 Load  
Course Type: Occupational

First Term: 2018 Fall  
Final Term: Current

Description: Managing Linux Operating Systems including sophisticated manipulation of file structures, backup systems, printing processes, troubleshooting, user account management, hard disk maintenance and configuration, process monitoring and prioritizing, kernel customization, and system resource control. Preparation for industry certifications such as the CompTIA Linux+, the Red Hat Certified System Administrator (RHCSA), the Red Hat Certified Engineer (RHCE) and the Linux Professional Institute (LPIC-1).

Requisites: Prerequisites: A grade of C or better in CIS126DL or CIS126RH or permission of Instructor.

MCCCD Official Course Competencies

1. Demonstrate understanding of Linux File System standards. (I)
2. Demonstrate the utilization of automated backup procedures. (I, IV, V, VI)
3. Manage and control system resources such as memory and CPU usage through a variety of techniques. (I, IV, VI)
4. Configure printing system to local and remote network printers including print job filtering and management. (I, IV, VI)
5. Create and implement a security policy including an emergency security plan. (I, II, III, V, VI)
6. Design fault-tolerant systems and network environments. (I, V, VI)
7. Customize system security through the use of user system profiles, user and group accounts, and file and directory privileges. (II, III, V, VI)
8. Create partitions and file systems and manipulate access to them through the use of mount points and automated mounting techniques. (II, IV, VI)
9. Recompile the kernel of the Linux operating system from source code and explain the benefits. (II, III)
10. Apply su and sudo commands to access administrative system privileges. (III)
11. Monitor system functions and security through the use of a variety of system logs. (III)
12. Add to repertoire of system prompt commands used to control the Linux operating system. (I, II, III, IV, V, VI)
13. Apply a variety of command line and graphical applications to perform a variety of user and administrative tasks. (V)
14. Implement a variety of troubleshooting techniques to prevent and deal with a variety of system problems including core dumps. (VI)

MCCCD Official Course Outline

https://artemis.mac2.az.edu/epj-bin/WebObjects/MCCCD.wss/ws/findForm2?id=123984
I. Theory of Operation
   A. File system hierarchy standards
   B. Cron daemon’s (task scheduling utility) implementation of file system backup
   C. System tuning
   D. Print process and the role of the Berkeley Software Distribution (BSD) printing model
   E. Common physical network problems and the troubleshooting measures
   F. Emergency measures when network vulnerabilities are breached
   G. Key system resources
   H. Redundant Array of Independent Disks (RAID) storage
II. Base System
   A. Key files used in configuring user profiles
   B. Adding and removing users
   C. Run levels and specific roles of reserved run levels 0, 1, and 6
   D. File system table configuration file (fstab) in mounting and unmounting file systems and devices
   E. Recompiling the kernel
III. Shells and Commands
   A. Switch user (su) command
   B. Message of the day (mood) and its role in user communication
   C. Microsoft Disc Operating System OS (MS-DOS) tools and their use in a Linux system
   D. Make command in the compilation of source code
   E. Function of the touch command and its effect on system logs
   F. System status, system message logging, and performance analysis
IV. System Services
   A. Function of common user commands
   B. Utilities used for archiving
   C. File system check command (fsck) and program’s default run time
   D. Process management and the options that accompany those commands
   E. Printer configuration options
   F. Line printer daemon and the foreground line printer requester
   G. Package managers utilizing software packages
V. Applications
   A. Backup applications
   B. Mail exchange programs
   C. Web server daemons
   D. Processor, system architecture and compiler design
   E. File Transfer Protocol (FTP) clients and servers
   F. Secure Shell (SSH) network
   G. Common graphical configuration tools
VI. Troubleshooting
   A. Tools, procedures, and techniques for administering a variety of systems within the Linux architecture
   B. Measures to prevent and control core dumps
   C. Rescue environment utilities

MCCCD Governing Board Approval Date: November 28, 2017

All information published is subject to change without notice. Every effort has been made to ensure the accuracy of information presented, but based on the dynamic nature of the curricular process, course and program information is subject to change in order to reflect the most current information available.
Information Security Fundamentals

Course: ITS110  Lec + Lab  3.0 Credit(s)  4.0 Period(s)  4.0 Load
Course Type: Occupational
First Term: 2020 Fall
Final Term: Current

Description: Fundamental concepts of information technology security. Topics include authentication methods, access control, cryptography, Public Key Infrastructure (PKI), network attack and defense methods, hardening of operating systems and network devices, securing remote access and wireless technologies and securing infrastructures and topologies. Emphasis on hands-on labs in both the Windows and Linux environments. Builds on thorough understanding of Transmission Control Protocol/Internet Protocol (TCP/IP) and security concepts and Microsoft (MS) Windows and Linux Administration.

Requisites: Prerequisites: A grade of C or better in CIS126DL, or CIS126RH, or permission of Program Director. Co-requisites: BPC270 or MST150++.

MCCCD Official Course Competencies

1. Explain the need for authentication methods and available solutions. (I)
2. Implement appropriate access control methods and demonstrate techniques for monitoring access to network resources. (II)
3. Apply cryptographic methods to ensure data integrity and privacy. (III)
4. Explain the elements of Public Key Infrastructure and how to plan for implementation. (IV)
5. Identify the types of threats to networks and the steps to take to reduce these threats. (V)
6. Identify vulnerabilities in operating system software and network devices, and implement measures to mitigate these vulnerabilities. (VI)
7. Demonstrate methods to secure remote access to network resources. (VII)
8. Identify weaknesses in wireless technology and implement measures to secure wireless environments. (VIII)
9. Explain the methods used to design and maintain a secure network infrastructure. (IX)
10. Explain the techniques used to assess risk, detect network intrusions and ensure the continuity of network resources. (X)
11. Describe the elements of effective security policies in a business environment. (XI)

MCCCD Official Course Outline

I. Authentication methods
   A. Security terms
   B. Central Intelligence Agency and non-repudiation
   C. Security standards
   D. Kerberos
   E. Certificates
   F. Token-based authentication

https://azmarccollege2.az.csdersobjects/MCCCD xdoc/az.htm?formid=145941
G. Challenge Handshake Authentication Protocol (CHAP)
H. Smart Cards
I. Biometrics
J. Extensible Authentication Protocol (EAP)

II. Access control
A. Access control terminology and concepts
B. Auditing and logging
C. Isolating the auditing system
D. Filtering logs
E. Audit trails and the collection of evidence
F. Access Control Methods Discretionary Access Control (DAC), Mandatory Access Control (MAC)
   and Role-Based Access Control (RBAC)
G. Balancing responsibilities of security

III. Cryptography
A. Cryptography and encryption
B. Common cryptography terms
C. Types of encryption algorithms
D. Services provided by encryption
E. Hash encryption
F. Symmetric-key encryption
G. Asymmetric-key encryption
H. Applied encryption

IV. Public Key Infrastructure (PKI)
A. PKI terms
B. Types of certificates
C. PKI standards and protocols
D. Public-Key Infrastructure X.509 (PKIX)
E. Certificate policies
F. Certificate Practice Statement (CPS)
G. Certificate revocation
H. Online Certificate Status Protocol (OCSP)
I. Trust models
J. Centralized and decentralized key management
K. Key management and certificate life cycles
L. Certificate and key storage
M. Planning for PKI

V. Network attacks and vulnerabilities
A. File Transfer Protocol/Internet Protocol (FTP/IP) protocol suite overview
B. Spoofing attacks
C. Scanning attacks
D. Denial-of-Service (DOS) attacks
E. Distributed Denial-of-Service (DDOS) attacks
F. Mitigating vulnerability and risk
G. Man-in-the-Middle attacks
H. Packet sniffling
I. TCP/IP Connection hijacking
J. Domain Name System (DNS) and Address Resolution Protocol (ARP) cache poisoning
K. Password-guessing attacks
L. Software exploitation
M. Back door
N. Weak keys
O. Birthday attack
P. Mathematical attacks
Q. Social Engineering
R. Hoaxes
S. Malicious code
T. Viruses
U. Worms
V. Illicit servers
W. Trojan horses and root kits
X. Logic bombs
Y. Managing malware
Z. Auditing, logging and system scanning

VI. Operating system and application hardening
A. Security baselines
B. Client security issues
C. Encryption: Secure Socket Layer (SSL) and Transport Layer Security (TLS)
D. Isolating services and jails
E. Mail servers and Simple Mail Transport Protocol (SMTP) relay
F. File sharing
G. File transfer vulnerabilities
H. Server Message Block (SMB) encryption
I. File Transfer Protocol (FTP)
J. Securing web servers
K. DNS servers
L. Data repositories
M. Operating system hardening

VII. Securing remote access
A. Concepts, terminologies and methods
B. Virtual Private Networks (VPNs)
C. Terminal Access Controller Access Control System (TACACS and TACACS+)
D. Remote Authentication Dial-In User Service (RADIUS)
E. Internet Protocol Security (IPSec)
F. 802.1x
G. Remote administration methods
H. Secure Shell (SSH)

VIII. Wireless network security
A. Wireless technologies
B. Wireless networking modes
C. Wireless cells
D. Wireless Application Protocol (WAP)
E. Wireless Transport Layer Security (WTLS)
F. Wireless Vulnerabilities and Wired Equivalent Privacy (WEP)
G. Solutions for wireless network vulnerabilities
H. Site surveys and war driving

IX. Securing topologies and infrastructure
A. Firewall overview
B. Security topologies
C. Security zones
D. Virtual Local Area Network (LAN) (VLAN)
E. Network Address Translation (NAT)
F. Traffic control methods
G. Configuring firewalls
H. Configuring an Access Control List (ACL)
I. Network device hardening
J. Physical security
K. Cabling and network security
X. Risk analysis, intrusion detection and business continuity
   A. Risk identification
   B. Intrusion detection systems
   C. Honey pots
   D. Incident response policy
   E. Forensics
   F. Disaster recovery plan
   G. Business continuity
XI. Security policy management
    A. Security policy
    B. Human resource policies
    C. Documentation

MCCCD Governing Board Approval Date: February 25, 2020

All information published is subject to change without notice. Every effort has been made to ensure the accuracy of information presented, but based on the dynamic nature of the curricular process, course and program information is subject to change in order to reflect the most current information available.
Ethics in Information Technology

Course: CIS111
Lecture 3 Credit(s) 3 Period(s) 3 Load
Course Type: Occupational

First Term: 2014 Fall
Load Formula: S - Standard
Final Term: Current

Description: Ethical issues that arise as a result of increasing use of computers, and the responsibilities of those who work with computers, either as computer science professionals or end users. Critical inquiry and review of ethical challenges in information technology business, including professional and corporate responsibility, government regulation, fiduciary responsibilities of information, infringement of intellectual property, security risk assessment, Internet crime, identity theft, employee surveillance, privacy, compliance, social networking, and the ethics of IT corporations.

Requisites: Prerequisites: None.

MCCCD Official Course Competencies

1. Describe a variety of different ethical theories. (I)
2. Describe professional business ethics and the complexities of making ethical judgments. (I)
3. Describe issues relating to corporate ownership, corporate governance, and responsiveness to corporate stakeholders. (II)
4. Explain how social media responsibility encompasses economic, legal, ethical, and privacy issues. (II)
5. Explain whistle-blowing and protection for whistle-blowers. (II)
6. Describe the major ethical challenges of operating in a healthcare environment using mobile and wireless technologies. (II)
7. Explain fiduciary responsibilities of private information. (II)
8. Describe issues with software and software liability. (III)
9. Explain cost/benefit analysis in information technology ethical decision-making. (III)
10. Describe the influence of government regulations as well as professional self-regulation and sanctions in ethical information technology decision-making. (IV)
11. Explain intellectual property, copyright laws, and fair use doctrine. (IV)
12. Define hate speech and defamation. (V)
13. Review contemporary issues related to workplace monitoring. (V)
14. Describe the major identity theft issues. (V)
15. Describe Information Technology security breaches and risk assessments. (V)
16. Define security policies within Information Technology. (V)
17. Describe professional codes of ethics for Information Technology professionals. (V)
18. Describe prevention, detection, and responses to Information Technology security attacks. (V)

MCCCD Official Course Outline

I. Ethics and Ethical Theories
   A. Sources of ethical theories

https://arizona.mac2.rr.com/WEBObjects/MCCCD.xos/wwHveForm2?id=74479
B. Definition of professional Information Technology ethics
C. Application of ethical theories to business

II. Corporate and Individual Responsibilities
A. Responsibilities to shareholders
B. Responsibilities to stakeholders
C. Social media responsibility
D. Healthcare information privacy issues with mobile and wireless technologies
E. Fiduciary responsibilities concerning private information
F. Whistle-blower rights and responsibilities

III. Obligations in the Information Technology Profession
A. Describe liabilities related to software
B. Give examples of secure coding
C. Give examples of cost/benefit analysis in information technology ethical decision-making

IV. Decision-Making in Information Technology
A. Describe the influence of government regulations and professional self-regulation The professional and corporate social audit
B. Describe intellectual property, copyright laws, and fair use doctrine

V. Application of Ethics to Specific Areas of Information Technology
A. Explain hate speech and defamation
B. Explain privacy issues related to workplace monitoring
C. Give examples of Information Technology security breaches and risk assessments
D. Define security policies within Information Technology
E. Describe prevention, detection, and responses to Information Technology security attacks
F. Describe the major identity theft issues
G. Describe the professional code of ethics for Information Technology professionals

MCCCD Governing Board Approval Date: June 24, 2014

All information published is subject to change without notice. Every effort has been made to ensure the accuracy of information presented, but based on the dynamic nature of the curricular process, course and program information is subject to change in order to reflect the most current information available.
Python Programming: Level I

Course: CIS 156
Lec + Lab: 3.0 Credit(s) 4.0 Period(s) 4.0 Load
Course Type: Occupational
Load Formula: T + Lab Load
First Term: 2021 Fall
Final Term: Current

Description: Introduction to Python programming. Includes general concepts, program design, development, data types, operators, expressions, flow control, functions, classes, input and output operations, debugging, structured programming, and object-oriented programming.

Requisites: Prerequisites: A grade of C or better in CIS 105 or permission of Instructor.

MCCCD Official Course Competencies

1. Explain the development of Python applications. (I)
2. Explain the control structures in Python. (II)
3. Utilize basic data structures in Python. (III, IV)
4. Utilize string and character manipulation in Python. (V)
5. Utilize object-oriented programming concepts in Python. (VI)
6. Utilize Python to load, save and manipulate persistent data. (VII)
7. Identify and debug common mistakes in programs written in Python. (VIII, IX)

MCCCD Official Course Outline

I. Python language
   A. History of Python
   B. Operators
   C. Variables
   D. Terminology
   E. Selection structure

II. Control structures/statements
   A. Counter-controlled repetition
   B. For repetition
   C. While repetition
   D. Break and Continue statements

III. Functions
   A. Program functions in Python
   B. Class methods
   C. Using Python modules
   D. Recursion vs. iteration

IV. Data structures operations
   A. Lists
   B. Tuples
   C. Dictionaries

https://sas.mesa.edu/gp-bin/WebObjects/MCCCD.wa.os/form1?id=163971

1/2
D. Sets  
E. Range  
V. String and characters  
A. Fundamentals of characters and strings  
B. String constructors  
C. Concatenating strings  
D. String methods  
VI. Object-oriented programming  
A. Definition  
B. Class scope and access  
C. Constructors/Methods  
D. Abstraction  
E. Software reusability  
F. Encapsulation  
G. Inheritance  
H. Composition  
VII. Data persistence  
A. Read and write text data to text files  
B. Support of database connectivity  
C. Issue embedded SQL commands (SELECT/UPDATE/INSERT/DELETE) via Python  
VIII. Debugging  
A. Syntax errors  
B. Logic errors  
C. Run-time errors  
D. Debugging techniques  
E. Test data  
IX. Exception handling  
A. The basics of Python error-handling  
B. Error-handling techniques  
C. Try blocks  
D. Throwing, catching, and re-throwing an exception  

MCCCD Governing Board Approval Date: February 23, 2021  

All information published is subject to change without notice. Every effort has been made to ensure the accuracy of information presented, but based on the dynamic nature of the curricular process, course and program information is subject to change in order to reflect the most current information available.
Intro to Computer Systems
- MS Office Apps
- Internet access
- eBook curriculum

Hardware / Software Lab Setup
- Lab Tables w/integrated power
- Anti-Static Mat on the tables
- eBook curriculum
- Packet Tracer software

Computer Kit – the kit requirements will vary upon how you choose to allow students to connect for the purpose of downloading OS and various drivers (PacketTracer is now on the approved software list)

<table>
<thead>
<tr>
<th>Component</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Motherboard – ATX (full size)</td>
<td>31</td>
</tr>
<tr>
<td>a. LGA1200 – Intel</td>
<td></td>
</tr>
<tr>
<td>2. CPU w/heat sink &amp; fan</td>
<td>31</td>
</tr>
<tr>
<td>3. Graphics Processing Card</td>
<td>31</td>
</tr>
<tr>
<td>4. RAM (8GB) - recommended by Cisco (2 X 4GB suggested)</td>
<td>31</td>
</tr>
<tr>
<td>needed for VM practice in curriculum</td>
<td></td>
</tr>
<tr>
<td>5. Case (ATX)</td>
<td>31</td>
</tr>
<tr>
<td>6. Ethernet Card</td>
<td>31</td>
</tr>
<tr>
<td>7. PCI / PCIe</td>
<td>31</td>
</tr>
</tbody>
</table>

This storage setup will allow students to configure their machine and NOT have to reverse all their work for the next class. Each student would be assigned an SSD that would remain in the classroom and used for their work in the lab

<table>
<thead>
<tr>
<th>Component</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>8. Storage</td>
<td></td>
</tr>
<tr>
<td>a. Swappable SSD</td>
<td></td>
</tr>
<tr>
<td>i. Bay (30) - ~$25/e (CDW)</td>
<td>31 Bays</td>
</tr>
<tr>
<td>ii. Trays (1 for each student) - ~$11/e (CDW)</td>
<td>1/Tray per SSD</td>
</tr>
<tr>
<td>b. SSD – 120GB (1 for each student) - ~$30/e (CDW)</td>
<td>1/per student</td>
</tr>
</tbody>
</table>
Cables
- Ethernet UTP bulk cable (CAT5e)
- Stranded UTP bulk cable (CAT5e)
- RJ45 connectors – Stranded and Solid Core
- RJ45 Network Cable Tester
- Crimpers
- Multimeter
- Networking scissors
- Cable stripper
- PC Power Supply Tester
- Anti-Static Duster
- Network Cable Tester

Tools
- 11-piece PC computer tool kit
- Anti-static wrist strap

Printer
Switch / Router
HDMI Monitors

ULINE Search Results: Stainless Steel Mobile Security Cage
# Basha High School Lab Tool Inventory

<table>
<thead>
<tr>
<th>Item</th>
<th>Qty</th>
<th>Vendor</th>
<th>Picture</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Multimeter, MSR-C600</td>
<td>2</td>
<td>Amazon</td>
<td><img src="image" alt="Digital Multimeter" /></td>
<td>$49.98</td>
</tr>
<tr>
<td>PC Power Supply Tester</td>
<td>2</td>
<td>Amazon</td>
<td><img src="image" alt="PC Power Supply Tester" /></td>
<td>$36.38</td>
</tr>
<tr>
<td>11 Piece PC Computer Tool Kit</td>
<td>31</td>
<td>Amazon</td>
<td><img src="image" alt="11 Piece PC Tool Kit" /></td>
<td>$827.08</td>
</tr>
<tr>
<td>Anti-Static Wrist Strap</td>
<td>5</td>
<td>Amazon</td>
<td><img src="image" alt="Anti-Static Wrist Strap" /></td>
<td>$59.95</td>
</tr>
<tr>
<td>MetroVac Anti-Static Electric Duster</td>
<td>2</td>
<td>Amazon</td>
<td><img src="image" alt="MetroVac Anti-Static Duster" /></td>
<td>$259.98</td>
</tr>
<tr>
<td>Cable Crimpers RJ45 Crimp</td>
<td>30</td>
<td>Amazon</td>
<td><img src="image" alt="Cable Crimpers RJ45 Crimp" /></td>
<td>$419.70</td>
</tr>
<tr>
<td>RJ45 Connectors SHD CAT6 Solid/Stranded Core</td>
<td>10</td>
<td>Amazon</td>
<td><img src="image" alt="RJ45 Connectors" /></td>
<td>$144.90</td>
</tr>
<tr>
<td>Item Description</td>
<td>Quantity</td>
<td>Supplier</td>
<td>Unit Price</td>
<td>Total Cost</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>NavePoint CAT5e, Solid Bulk Ethernet Cable UTP</td>
<td>1</td>
<td>Amazon</td>
<td>$56.42</td>
<td>$56.42</td>
</tr>
<tr>
<td>Belkin 250 ft CAT5e Stranded UTP Bulk Networking Cable</td>
<td>1</td>
<td>Amazon</td>
<td>$63.03</td>
<td>$63.03</td>
</tr>
<tr>
<td>RJ45 Network Cable Tester for LAN Phone/RJ45 WireTestTool</td>
<td>30</td>
<td>Amazon</td>
<td>$299.70</td>
<td>$299.70</td>
</tr>
<tr>
<td>Networking Scissors</td>
<td>5</td>
<td>Amazon</td>
<td>$99.85</td>
<td>$99.85</td>
</tr>
<tr>
<td>Network Cable Tester</td>
<td>1</td>
<td>Amazon</td>
<td>$22</td>
<td>$22</td>
</tr>
<tr>
<td>Mini Wire Stripper</td>
<td>1</td>
<td>Amazon</td>
<td>$8</td>
<td>$8</td>
</tr>
<tr>
<td><strong>Total Cost</strong></td>
<td></td>
<td></td>
<td><strong>$2,346.97</strong></td>
<td><strong>$2,346.97</strong></td>
</tr>
</tbody>
</table>
Cisco CCN 200-301 Standard Kit

Hardware included:
- These Cisco 1941 256/64 Routers (Dual FE router supports ISL/4 Advanced IP Services)
- These Cisco 2960-TF-L Switches (Supports ISL/2 ISLs) and IPv6 addressing and can do very limited Layer 3 static routing.
- These Ethernet Patch Cables
- These Ethernet Crossover Cables
- Cisco Console Kit
- Power Cords

Additional items included:
- 450 Page CCNA 200-301 Lab eWorkbook Covering 60+ Labs Plus Bonus Labs That Go Beyond the Scope of CCNA For Extra Real World Experience ($57.99 value)
- 864 Page Bootcamp & Theory eBook that covers every 200-301 CCNA Topic Plus More! ($49.99 value)
- How & Why We Subnet eWorkbook ($24.99 value)
- Two Practice Exams. Both with 101 Questions, Answers and Explanations ($15.99 value)
- CCNA CBAM Sheet ($14.99 value)
- TCP/IP Study Poster ($9.99 value)
- CertificationKits TFTP Server
- CertificationKits Subnet Calculator
- CertificationKits Binary Bits Game
- 50 CCNA Instructional Videos
- Cisco Network Assistant
- Cisco Router Password Decryptor
- Cisco VPN Client 5.0.04.0410
- Port Scanner nmap-7.30
- nmap-6.99beta7 & WinPcap 4.1.3
- WireShark 1.10.0, 1.2.2
- TerraTerm & Putty Terminal Emulators
- VirtualBox 6.1.4
- IOS Backup as noted above for the routers and switches
- Cisco Configuration Professional (CCP) 2.8 for 1941/2960 Series Routers
<table>
<thead>
<tr>
<th>QUANTITY</th>
<th>CAT NO.</th>
<th>DESCRIPTION</th>
<th>UNIT PRICE</th>
<th>TOTAL AMOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td></td>
<td>CCNA Standard 200-301 Kit</td>
<td>459.99</td>
<td>1,839.96</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Mini 12U Deluxe Rack &amp; Rack Kits</td>
<td>139.99</td>
<td>559.96</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Smart Serial Bundle</td>
<td>150.00</td>
<td>600.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

**SUBTOTAL** 2,999.92

https://shop.certificationkits.com/cisco-ccna-200-301-standard-kit/
Certification Kits
1212 S Naper Blvd Ste 119-329
Naperville
60540

Billing Details

<table>
<thead>
<tr>
<th>Order:</th>
<th>#36468</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment Method:</td>
<td>Check/Wire/Phone ($3,638.84)</td>
</tr>
</tbody>
</table>

Shipping Details

<table>
<thead>
<tr>
<th>Order Date:</th>
<th>Jan 19th 2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shipping Method:</td>
<td>UPS</td>
</tr>
</tbody>
</table>

Order Items

<table>
<thead>
<tr>
<th>Qty</th>
<th>Code/SKU</th>
<th>Product Name</th>
<th>Price</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>SKU-3020</td>
<td>Cisco CCNA 200-301 Standard Kit</td>
<td>$779.97 USO</td>
<td>$3,119.88 USO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rack Options:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Min 12U Deluxe</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rack &amp; Rack Kits (+ $139.99)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional Serial Cards and Cables Bundle:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Smart Serial Bundle (+ $150.00)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supplemental CCNA Training DVD:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional Wireless Access Point:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FTDI Console Cable Upgrade:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>One-Time Print Right for Lab Workbook:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Extended Warranty:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 Year (included)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>SKU-2727</td>
<td>9 Outlet POU</td>
<td>$34.99 USO</td>
<td>$139.98 USO</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Subtotal:</td>
<td></td>
<td>$3,259.84 USO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Shipping:</td>
<td></td>
<td>$379.00 USO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Grand Total:</td>
<td></td>
<td>$3,638.84 USD</td>
</tr>
</tbody>
</table>


# Arizona Department of Education CTE Recommended Equipment List

## Career and Technical Education

### Recommended Equipment List

**Program:** NETWORK SECURITY  
**CIP#:** 11.1999.00

**NOTE:** The following items and descriptions are the recommended equipment guidelines for each CTE Network Security program. Please note that this list of recommended items does not necessarily need to be supported financially by Federal Perkins or State Priority funding sources. In many cases, local school district funds are used to purchase items on a regular basis (i.e., furniture, consumables, etc.). Further, please understand that this is not an exhaustive list. Local program and business needs may necessitate the purchase of additional equipment and software resources, as may the rapidly-changing nature of the industry-specific technologies used in the program.

Please contact ADE-CTE Program Specialist Tracy Rexroat (tracy.rexroat@azed.gov) if you have questions regarding the appropriateness of any item you are considering for addition to your CTE Network Security program.

<table>
<thead>
<tr>
<th>Item</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cable Cutter, Coax</td>
<td>30</td>
</tr>
<tr>
<td>Crimp Tool W/ Stripper, RJ11, RJ45</td>
<td></td>
</tr>
<tr>
<td>File, Flat Needle</td>
<td></td>
</tr>
<tr>
<td>Flashlight, Tactical L.E.D.</td>
<td>5</td>
</tr>
<tr>
<td>Forceps, Straight w/Grip</td>
<td></td>
</tr>
<tr>
<td>Handle, For Blades, Drive-Loc</td>
<td>2</td>
</tr>
<tr>
<td>Hex Keys Set, Fold-Up .050” to 3/16”</td>
<td></td>
</tr>
<tr>
<td>Insertion/Extraction Tool</td>
<td></td>
</tr>
<tr>
<td>Nutdriver Blade, 3/16&quot; 1/4, 5/16, 3/8</td>
<td></td>
</tr>
<tr>
<td>Pliers, Diagonal 4” W/Spring</td>
<td></td>
</tr>
<tr>
<td>Pliers, Long Nose 4 3/4”, 6” w cutter</td>
<td></td>
</tr>
<tr>
<td>Pliers, Slip Joint 6”</td>
<td></td>
</tr>
<tr>
<td>Pliers, Vise-Grip Long Nose 6”</td>
<td>5</td>
</tr>
<tr>
<td>Punchdown Tool W/110 Blade</td>
<td></td>
</tr>
<tr>
<td>Receptacle Analyzer</td>
<td></td>
</tr>
<tr>
<td>Screwdriver, Phillips #0 x 2”, 1x3, 2x4</td>
<td>30</td>
</tr>
<tr>
<td>Screwdriver, Slot 1/4” x 6”</td>
<td></td>
</tr>
<tr>
<td>Screwdriver, Slot 3/16” x 4”</td>
<td></td>
</tr>
<tr>
<td>Screwdriver, Slot 3/32” x 2”</td>
<td></td>
</tr>
<tr>
<td>Screwdriver, Stubby 2 in 1</td>
<td></td>
</tr>
<tr>
<td>Soldering Iron, 25 Watt 3-wire</td>
<td>3</td>
</tr>
<tr>
<td>Telephone Line Tester</td>
<td></td>
</tr>
<tr>
<td>Tone Line Aid W/Volume Control (Multimeters)</td>
<td></td>
</tr>
<tr>
<td>Tone Tracer, High Powered (Circuit Tracer)</td>
<td></td>
</tr>
<tr>
<td>Trimpot Tool</td>
<td></td>
</tr>
<tr>
<td>Wire Strippers, &quot;T&quot; 18-28 (1)</td>
<td></td>
</tr>
<tr>
<td>Wrench, Adjustable 6” Ergonomic</td>
<td></td>
</tr>
<tr>
<td>Desktops/ Laptops/ or I-pads</td>
<td>31</td>
</tr>
<tr>
<td>Routers</td>
<td>12</td>
</tr>
<tr>
<td>Servers</td>
<td>2</td>
</tr>
<tr>
<td>Switches</td>
<td>12</td>
</tr>
<tr>
<td>Software tools for Analysis</td>
<td></td>
</tr>
<tr>
<td>Network protocol analyzer, e.g. TShark, iPerf3 to support tuning of many parameters buffers, and protocols (TCP, UDP, SCTP with IPv4 and IPv6)</td>
<td>Wireshark and Packet Tracer</td>
</tr>
<tr>
<td>Security scanner to create a map of the network.</td>
<td></td>
</tr>
<tr>
<td>Debugger program to find communication and/or data problems in SNMP monitoring configurations.</td>
<td></td>
</tr>
<tr>
<td>IP address and port scanner.</td>
<td></td>
</tr>
<tr>
<td>IP calculator</td>
<td></td>
</tr>
</tbody>
</table>

---

**Arizona Department of Education**  
**Career and Technical Education**  
**Network Security**  
**Date:** 6/16/2021
**Monitoring & Logging**

- Network monitoring software solution to dig deep into the health and integrity of your systems and network. An approach to monitoring.
- System usage software.

**NetFlow Analyzer**
- Server software: Red Hat, Ubuntu, MS Server, AWS Cloud, VMWare
- Configuration & Transfer software: Clonezilla, Terra Term, putTY, UDP Cast
- A multi-vendor Python library: Internet access to IP & PMP Modules
- Network device software: Firmware access for devices
- Platform supports: Operating system keys for each student
- TFTP Server: Can be installed on server software
- SFTP/SCP Server software: Can be installed on server software

For Network troubleshooting: https://www.pluralsight.com/blog/it-ops/network-troubleshooting-tools

Free tools: https://www.networkmanagementsoftware.com/top-17-free-tools-for-network-administrators/

- Sensors: pressure, magnetic, resistive, capacitance, photo electric
- PLCs
- Motors
- Actuators
- Relays
- IC controllers
- Breadboard
- Switches
- Printed circuit boards PCBs
- Power supplies

**Programmable manipulators**

- 1 cartesian
- 2 gantry
- 3 cylindrical
- 4 spherical
- 5 articulated
- 6 SCARA

**Robot controls**

- 1 Point to point (PTP)
- 2 Continuous path control
- 3 Controlled path control

**Automation and programming control tools**

- Programmable Computer Numeric control
- Direct Numeric Control DNC
- Printed Circuit Boards (PCB’s)
- Computer-integrated manufacturing (CIM)
- HMI software
- PAC, PLC and controllers software

*Must meet the guidelines for specialized computing equipment as outlined on the "CTE Equipment Guidelines" at www.azed.gov/cte/grants*

**Additional Items:**

<table>
<thead>
<tr>
<th>Item</th>
<th>Quantity</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Scissors:</td>
<td>10</td>
<td>31</td>
</tr>
<tr>
<td>CAT6 Cable:</td>
<td>500 ft</td>
<td>31</td>
</tr>
<tr>
<td>RF45 Connectors:</td>
<td>1000</td>
<td>31</td>
</tr>
<tr>
<td>Network Patch Panel:</td>
<td>4</td>
<td>31</td>
</tr>
<tr>
<td>Anti-Static Electric Duster:</td>
<td>2</td>
<td>31</td>
</tr>
<tr>
<td>Anti-Static Wrist Strap:</td>
<td>30</td>
<td>31</td>
</tr>
<tr>
<td>PC Computer Tool Kit:</td>
<td>30</td>
<td>31</td>
</tr>
<tr>
<td>Digital Multimeter:</td>
<td>2</td>
<td>31</td>
</tr>
<tr>
<td>Computer Kit:</td>
<td>31</td>
<td>1</td>
</tr>
<tr>
<td>RAM:</td>
<td>31</td>
<td></td>
</tr>
</tbody>
</table>

**Arizona Department of Education**

**Career and Technical Education**

**Recommended Equipment List:**

**Network Security**

2 of 2

6/16/2021
Appendix K: Chandler High School Cyber Program Profile

Enrollment

<table>
<thead>
<tr>
<th>Academic Year</th>
<th>Grade 9</th>
<th>Grade 10</th>
<th>Grade 11</th>
<th>Grade 12</th>
<th>Total</th>
<th>Graduates</th>
</tr>
</thead>
<tbody>
<tr>
<td>2022 – 2023</td>
<td>17</td>
<td>34</td>
<td>12</td>
<td>19</td>
<td>82</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2022 – 2023 School Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grade Level</td>
</tr>
<tr>
<td>9th</td>
</tr>
<tr>
<td>10th</td>
</tr>
<tr>
<td>11th</td>
</tr>
<tr>
<td>12th</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

Demographics

<table>
<thead>
<tr>
<th>Diversity</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>White</td>
<td>19%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hispanic / Latino</td>
<td>41%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Asian or Asian / Pacific Islander</td>
<td>10%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Black or African American</td>
<td>10%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>American Indian or Alaska Native</td>
<td>2%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other or Undeclared</td>
<td>18%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Minority Enrollment</td>
<td>63%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Gender           | Male    | 67      |          |          |        |          |
|                 | Female  | 15      |          |          |        |          |

| Student to Teacher Ratio | 20:1 |

Operations

Personnel

<table>
<thead>
<tr>
<th>Teacher</th>
<th>Education Level</th>
<th>Certifications</th>
<th>Years of Experience</th>
<th>Courses Taught</th>
<th>Dual Enrollment Qualified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Janet Hartkopf</td>
<td>MS Curriculum &amp; Instruction - Technology</td>
<td>CTE Certified</td>
<td>11 Years</td>
<td>Security Fundamentals Ethics in IT</td>
<td>Y</td>
</tr>
<tr>
<td>Mathews, Jonah</td>
<td>BS Education</td>
<td>CTE Certification in Progress</td>
<td>2 Years</td>
<td>Hardware and Software CYB 120 – Introduction to Computer Systems</td>
<td>N</td>
</tr>
</tbody>
</table>

Equipment

<table>
<thead>
<tr>
<th>Equipment Type</th>
<th>Make</th>
<th>Model</th>
<th>Quantity</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Kit</td>
<td>Chandler HS Equipment Proposal 2022</td>
<td>31</td>
<td>$25,000</td>
<td></td>
</tr>
<tr>
<td>Misc. Tools</td>
<td>Chandler HS Lab Tool Proposal 2022</td>
<td>N/A</td>
<td>$2,346.97</td>
<td></td>
</tr>
<tr>
<td>Locking Storage</td>
<td>ULINE</td>
<td>H-6839</td>
<td>1</td>
<td>$1,300</td>
</tr>
<tr>
<td>PCs &amp; Monitors</td>
<td>“Chromebook” type laptop with ability to use PacketTracer</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Network
- Chandler Unified School District provided network access.
- Isolated network provided for cybersecurity classrooms and lab spaces.
  - Requires separate hardware and non-district issued machines.
  - Allows access websites, resources, and facilitates meeting the learning objectives of courses.

Facilities
- School has dedicated classroom space for cybersecurity program.
  - One general purpose classroom and one Career and Technical Education (CTE) Lab.
    - CTE lab space provides larger footprint. Consists of teaching space and space for hands on activities and equipment storage.
    - Classrooms have webcams and in-classroom microphones (2) to support video-conferencing capabilities.

Formal Learning Activities

<table>
<thead>
<tr>
<th>Course</th>
<th>Company</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYB 240A / CNT 140 – Intro to LAN &amp; Security Fundamentals</td>
<td>Cisco</td>
<td>* Free Courseware</td>
</tr>
<tr>
<td>CYB 240B / CNT 150 – Intro to LAN &amp; Security Fundamentals</td>
<td>Cisco</td>
<td>* Free Courseware</td>
</tr>
<tr>
<td>CYB 300A / CIS 126DL – Linux OS</td>
<td>Cisco</td>
<td>$30 per student lab fee</td>
</tr>
<tr>
<td>CYB 300B / CIS 238DL – Advanced Linux</td>
<td>Cisco</td>
<td>$30 per student lab fee</td>
</tr>
<tr>
<td>CYB 400A / CIS 110 – Information Security Fundamentals</td>
<td>TestOut</td>
<td>$2,900 per year (50 user license)</td>
</tr>
<tr>
<td>CYB 400B / CIS 111 – Ethics in Information Technology</td>
<td>Cengage</td>
<td>$4,620 for Print Student Edition + 6 years access to online platform MindTap x 40 (price includes shipping and processing)</td>
</tr>
<tr>
<td>CYB 130 / CIS 156 – Python</td>
<td>Cisco</td>
<td>* Free Courseware</td>
</tr>
</tbody>
</table>

- Program was modeled off the cybersecurity program at Basha High School (BHS).
- Leveraged Basha High School curriculum and pathways to Chandler Gilbert Community College (CGCC).
- Reverse engineered from Chandler Gilbert Community College (CGCC) four year plan to ensure articulation and pathway for students.
- Completing first year of the program in School Year 2022 – 2023. Courses will be scaffolded in as students advance through the program.
  *CYB 300 A / CIS 126DL – Linux OS will not be taught in School Year 2023 – 2024 (Year 2) due to teacher shortage.

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Syllabus</th>
<th>Dual Enrollment</th>
<th>Pre-Existing</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYB 120 / CIS 105 – Introduction to Computer Systems</td>
<td>Overview of computer technology, concepts, terminology, and the role of computers in business and society. Discussion of social and ethical issues related to computers. Use of word processing, spreadsheet, database, and presentation software. Includes uses of application software and the Internet for</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Course Code</td>
<td>Course Title</td>
<td>Description</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------</td>
<td>-------------</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>CYB 230 A / BPC 170 – Hardware and Software Config &amp; Support</td>
<td>This course provides an excellent introduction to the IT industry and interactive exposure to personal computers, hardware, and operating systems. Students participate in hands-on activities and lab-based learning to become familiar with various hardware and software components and discover best practices in maintenance and safety.</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>CYB 230 B / BPC 270 – Hardware and Software Config &amp; Support</td>
<td>This course provides an excellent introduction to the IT industry and interactive exposure to personal computers, hardware, and operating systems. Students participate in hands-on activities and lab-based learning to become familiar with various hardware and software components and discover best practices in maintenance and safety.</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>CYB 240 A / CNT 140 – Intro to LAN &amp; Security Fundamentals</td>
<td>This course teaches the fundamentals of networking. It covers how devices communicate on a network, network addressing and network services, how to build a home network and configure basic security, the basics of configuring Cisco devices, and testing and troubleshooting network problems.</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>CYB 240 B / CNT 150 – Intro to LAN &amp; Security Fundamentals</td>
<td>This course teaches the fundamentals of networking. It covers how devices communicate on a network, network addressing and network services, how to build a home network and configure basic security, the basics of configuring Cisco devices, and testing and troubleshooting network problems.</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>CYB 300 A / CIS 126DL – Linux OS</td>
<td>Introduction to the Linux Operating system. Develop knowledge and skills required to install, configure, and troubleshoot a Linux-based workstation including basic network functions. Learn basic command line and Graphical User Interface (GUI) desktop environment utilities and applications. Fundamental abilities to achieve the entry-level industry certification covered.</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>CYB 300 B / CIS 238DL – Advanced Linux</td>
<td>Managing Linux Operating Systems including sophisticated manipulation of file structures, backup systems, printing processes, troubleshooting, user account management, hard disk maintenance and configuration, process monitoring and prioritizing, kernel customization, and system resource control. Preparation for industry certifications such as the CompTIA Linux+, the Red Hat Certified System Administrator (RHCSA), the Red Hat Certified Engineer (RHCE) and the Linux Professional Institute (LPIC-1).</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>CYB 400A / CIS 110 -</td>
<td>Fundamental concepts of information technology security. Topics include</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>
### Information Security Fundamentals

| Authentication methods, access control, cryptography, Public Key Infrastructure (PKI), network attack and defense methods, hardening of operating systems and network devices, securing remote access and wireless technologies, and securing infrastructures and topologies. Emphasis on hands-on labs in both the Windows and Linux environments. Builds on thorough understanding of TCP/IP and security concepts and Microsoft (MS) Windows and Linux Administration. |
|---|---|---|
| CYB 400B / CIS 111 – Ethics in Information Technology | Ethical issues that arise because of increasing use of computers, and the responsibilities of those who work with computers, either as computer science professionals or end users. Critical inquiry and review of ethical challenges in information technology business, including professional and corporate responsibility, government regulation, fiduciary responsibilities of information, infringement of intellectual property, security risk assessment, Internet crime, identity theft, employee surveillance, privacy, compliance, social networking, and the ethics of IT corporations. | Y | Y | N |
| CYB 130 / CIS 156 - Python | Introduction to Python programming. Includes general concepts, program design, development, data types, operators, expressions, flow control, functions, classes, input, and output operations, debugging, structured programming, and object-oriented programming. | Y | Y | N |

### Non-Formal Learning Activities

| Camps | • AZ Cyber Initiative  
 • CyberPatriot |
|---|---|
| Certifications | • A+  
 • ITF+  
 • Linux+  
 • Security Pro  
 • Security+  
 • Python PCEP |
| Internships | • Open Source Integrators |
| Externships | • ElevateEd AZ  
 • Cybersecurity and Technology Externship |

### Informal Learning Activities

<table>
<thead>
<tr>
<th>Clubs</th>
<th>• Future Business Leaders of America (FBLA)</th>
</tr>
</thead>
</table>
| Competitions | • National Cyber League  
 • CyberPatriot |
Students are provided a variety of resources for additional learning outside of the classroom. Examples include cyber.org range access, Professor Messer videos, YouTube videos, and other resources.

<table>
<thead>
<tr>
<th>Conferences</th>
<th>CactusCon</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>WiCYS</td>
</tr>
<tr>
<td></td>
<td>K12 NICE Conference – Student Signing Day</td>
</tr>
<tr>
<td></td>
<td>Embry Riddle Aeronautical Engineering Cyber Day</td>
</tr>
<tr>
<td>Industry Events</td>
<td>PhoenixNap Tour</td>
</tr>
</tbody>
</table>

**Pathways**

<table>
<thead>
<tr>
<th>Post-Secondary</th>
<th>Chandler Gilbert Community College (CGCC) Cybersecurity AAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trade or Certification Program</td>
<td>Advanced Business Learning (ABL)</td>
</tr>
<tr>
<td>Military</td>
<td>Air Force JROTC</td>
</tr>
<tr>
<td>Workforce</td>
<td>Kelly Technologies</td>
</tr>
</tbody>
</table>
Survey of Computer Information Systems

Course: CIS105  Load + Lab  3.0 Credit(s)  4.0 Period(s)  4.0 Load
First Term: 2018 Fall  Course Type: Occupational
Final Term: Current  Load Formula: T

Description: Overview of computer technology, concepts, terminology, and the role of computers in business and society. Discussion of social and ethical issues related to computers. Use of word processing, spreadsheet, database, and presentation software. Includes uses of application software and the Internet for efficient and effective problem solving. Exploration of relevant emerging technologies.

Requisites: None.

Course Attributes:
General Education Designation: Computer/Statistics/Quantitative Applications - [CS]
Arizona Shared Unique Number SUN#: CIS 1120

MCCCD Official Course Competencies

1. Identify common hardware components of computer systems and describe their uses. (I)
2. Identify different types of software and their uses. (II)
3. Describe common uses of networks. (III)
4. Describe Web site Technology. (IV)
5. Use the Internet to communicate, collaborate, and retrieve information. (IV, VII)
6. Explore system security and privacy issues. (III, IV, VII)
7. Create macros and understand the basics of Visual Basic for Applications (VBA). (V)
8. Describe the steps in planning and implementing technology solutions. (VI)
9. Determine when technology is useful and select the appropriate tool(s) and technology resources to address a variety of tasks and problems. (VI, VIII)
10. Identify terminology and the uses of technology in business and society, including limitations. (VI)
11. Identify positive social and ethical behaviors when using technology and the consequences of misuse. (VII)
12. Describe how technology is used in the departments of a business and in various career paths. (VIII)
13. Use word processing, spreadsheet, database, and presentation software. (IX)

MCCCD Official Course Outline

I. Hardware
   A. Processing Unit
   B. Storage Devices
   C. Input Devices
   D. Output Devices

   (Not listed in the outline)

https://arizona.maricopa.edu/cej/bm/WebObjects/MCCCD.waa/wa/freeForm2?id=128924
E. Expansion Slots and Cards

II. Software
   A. System Software
      1. Operating System
      2. Utilities
      3. Device Drivers
   B. Application Software
      1. Word Processing
      2. Spreadsheets
      3. Databases
      4. Presentation Software
   C. Specialized Application Software
   D. Web Authoring Application Software

III. Networks
   A. Types of Networks
      1. Local Area Network (LAN)
      2. Wide Area Network (WAN)
   B. Uses of Networks
      1. Sharing Resources
      2. Communication
   C. Security and Data Integrity

IV. Internet
   A. History
   B. World Wide Web Structure
   C. Browsers
   D. Search Engines
   E. E-mail
   F. e-Commerce
   G. Hypertext Markup Language (HTML)
   H. Security
   I. Intranet
   J. Websites

V. Visual Basic Application (VBA)
   A. Visual Basic Editor
      1. Procedures
      2. Variables
   B. Macros
      1. Excel
      2. Access

VI. Planning and Implementing Technology Solutions
   A. Information Systems Role in Business
   B. Purchasing and Upgrading Microcomputers

VII. Social and Ethical Issues
   A. Ethics
   B. Viruses
   C. Security
   D. Ergonomics
   E. Intellectual Property Rights
   F. Privacy
   G. Green Computing

VIII. Uses of Technology
   A. Business
B. Career Paths

IX. Business Application Tools
A. Word
   1. Editing and formatting
   2. Creating and modifying
      a. Styles
      b. Table of Contents
      c. Index
B. PowerPoint
   1. Create and modify
      a. Slideshows
      b. Templates
      c. Outlines
C. Excel
   1. Create, edit, and format spreadsheets
   2. Create and modify formulas
   3. Use Excel functions
   4. Create and modify charts
   5. Table Management
      a. Sort
      b. Filter
      c. Import data
      d. Database functions
      e. Create, refresh, and delete
         (1) Pivot tables
         (2) Pivot charts
D. Access
   1. File management
      a. Design data
      b. Create tables
   2. Manage data
      a. Filter
      b. Sort
      c. Query
      d. Report
      e. Pivot table
         (1) View
         (2) Chart
      f. Structured Query Language (SQL)

MCCCD Governing Board Approval Date: 5/25/2010

All information published is subject to change without notice. Every effort has been made to ensure the accuracy of information presented, but based on the dynamic nature of the curricular process, course and program information is subject to change in order to reflect the most current information available.
A+ Exam Prep: Computer Hardware Configuration and Support

Course: BPC170  
Lec + Lab 3.0 Credit(s) 4.0 Period(s) 4.0 Load  
Course Type: Occupational  
First Term: 2020 Fall  
Final Term: Current  
Load Formula: T - Lab Load

Description: Explore technical aspects of personal computers, including system components, installation, system configuration, peripheral devices, and notebooks. Emphasis placed on hardware installation, maintenance, mobile devices, and hardware troubleshooting. Helps prepare students for the CompTIA A+ examinations.

Requisites: Prerequisites: None.

MCCCD Official Course Competencies

1. Identify the fundamental principles of using personal computers. (I, II, III)
2. Identify, install, configure, optimize, and upgrade personal computer components using appropriate tools. (I, II, III)
3. Identify the fundamental principles of networks. (IV)
4. Identify and describe network hardware and network media and their uses in given scenarios. (IV)
5. Install, configure, and deploy wired and wireless networks using appropriate tools and network components based upon given scenarios. (IV)
6. Identify the fundamental principles of using laptops. (V)
7. Install, configure, optimize, and upgrade laptops using appropriate tools. (V)
8. Identify the fundamental principles of using printers. (VI)
9. Install, configure, maintain, and share printers based upon given scenarios. (VI)
10. Explain the theory, processes, and best practices for troubleshooting hardware components, peripherals, mobile devices, and networking. (VII)
11. Identify symptoms and use the tools needed to fix hardware components, peripherals, mobile devices, and networking based upon given scenarios. (VII)

MCCCD Official Course Outline

I. Personal computers and components
   A. Connection interfaces and their purposes
      1. Serial, parallel, PS/2
      2. Universal Serial Bus (USB)
      3. IEEE 1394
   B. Components
      1. Cases
      2. Motherboards
      3. Processors
      4. Memory
      5. Expansion cards

https://aztransmac2.asu.edu/cgi-bin/WebObjects/MCCCD.woa/wa/freeForm2?id=153893
6. Power supplies
7. Cooling
C. Basic Input/Output System (BIOS) settings and security

II. Peripheral devices
A. Device connector types and associated cables
B. Display devices
   1. Analog
   2. Digital
   3. Multiple displays
C. Install drivers
D. Modify settings and properties

III. Storage
A. Storage devices
   1. Floppy disk
   2. Hard disk
   3. Optical discs
   4. Flash devices
   5. Solid state drives
   6. Tape drives
B. Connection types and associated cables
   1. Parallel ATA (PATA)
   2. Serial ATA (SATA)
   3. Small Computer System Interface (SCSI)
   4. USB/Firewire
   5. Ethernet
C. Redundant Array of Independent Discs (RAID)

IV. Networking
A. Network types
   1. Local Area Network (LAN)
   2. Wide Area Network (WAN)
   3. Personal Area Network (PAN)
   4. Metropolitan Area Network (MAN)
   5. Topologies
B. Network devices
   1. Network adapter
   2. Hub
   3. Switch
   4. Router
   5. Bridge
C. Network cables and connectors
   1. Coaxial
   2. Twisted pair
   3. Fiber optic
D. Network addressing
   1. Mac addresses
   2. Logical addresses
   3. Internet Protocol (IP) class
      a. Class A
      b. Class B
      c. Class C
   4. Static vs. dynamic
5. Client-Side Domain Name System (DNS)
6. Dynamic Host Configuration Protocol (DHCP)
7. Subnet mask
8. Gateway
E. Transmission Control Protocol (TCP) vs. User Datagram Protocol (UDP)
F. Common ports and protocols
G. Wireless networking
1. IEEE standards
2. Authentication
3. Security and encryption
H. Small Office/Home Office Network (SOHO)
V. Laptop devices
A. Hardware components and expansion options
B. Power saving options
C. Special function keys
D. Display technology
1. Liquid-Crystal Display (LCD)
2. Light-Emitting Diode (LED)
3. Organic Light-Emitting Diode (OLED)
4. Plasma
VI. Printing
A. Printer types
1. Ink jet (ink dispersion)
2. Laser
3. Thermal
4. Impact
B. Imaging processes
1. Electrophotographic (EP) process
2. Hewlett-Packard (HP) process
3. LED process
C. Sharing
D. Printer maintenance
VII. Hardware and network troubleshooting
A. Troubleshooting theory and methods
B. Hardware components
C. Video
D. Peripheral devices
E. Networking

MCCCD Governing Board Approval Date: June 23, 2020

All information published is subject to change without notice. Every effort has been made to ensure the accuracy of information presented, but based on the dynamic nature of the curricular process, course and program information is subject to change in order to reflect the most current information available.
A+ Exam Prep: Operating System Configuration and Support

Course: BPC270  Lec + Lab  3.0 Credit(s)  4.0 Period(s)  4.0 Load
Course Type: Occupational
First Term: 2018 Fall  Load Formula: T
Final Term: Current

Description: Explore advanced technical aspects of maintaining and servicing computers. Emphasis placed on OS installation, maintenance, mobile devices, security, software troubleshooting, and on proper usage of tools, safety procedures, and professionalism. Helps prepare students for the CompTIA A+ examinations.

Requisites: Prerequisites: A grade of C or better in CIS105 or permission of Instructor.

MCCCD Official Course Competencies

1. Identify the fundamentals of using operating systems. (I)
2. Install, configure, optimize, upgrade, and perform preventive maintenance on operating systems using appropriate tools, diagnostic procedures, and troubleshooting techniques. (I, II, VIII)
3. Explain the purposes, requirements, and security measurements needed for implementing virtualization. (III)
4. Define the different types of disk storage and file systems and perform common disk management and file management procedures. (IV, V)
5. Utilize common techniques for managing folders and files, including setting permissions, file attributes, sharing between users. (V)
6. Identify the fundamental principles of security. (VI)
7. Implement security policy and procedure on wired and wireless networks based upon given scenarios, including selection of appropriate security components. (VI)
8. Install, configure, upgrade, optimize and perform preventive maintenance with respect to security using appropriate tools, diagnostic procedures, and troubleshooting techniques. (VI)
9. Compare the differences between mobile devices, including hardware, mobile operating systems, and security. (VII)
10. Describe communication methods for mobile devices. (VII)
11. Setup, configure, and use applications to retrieve and synchronize data between a mobile device and computer/server. (VII)
12. Explain the processes and best practices for troubleshooting and fixing problems with operating systems and applications. (VIII)
13. Identify symptoms and use the tools needed to fix problems with operating systems and applications. (VIII)
14. Use job-related professional behavior including communication skills, tact, notion of privacy, confidentiality, and respect for the customer and customer’s property. (IX)
15. Explain safe lab procedures and tool use. (IX)
16. Describe potential safety hazards and safety procedures associated with a variety of computer equipment. (IX)
17. Describe the aspects and importance of safety and environmental issues including potential hazards and proper safety procedures with respect to computer maintenance. (IX)
I. Operating System (OS)
   A. Parts of an Operating System
      1. Kernel
      2. Drivers
      3. Interface
      4. Utilities
      5. Applications
   B. Components of Windows
      1. Desktop
      2. Taskbar
      3. Notification Area
      4. Windows Explorer
      5. Control Panel
      6. User Account Control (UAC)
      7. HomeGroup
   C. Components of Mac
      1. Desktop
      2. KeyChain
      3. Finder
      4. Dock
      5. Boot Camp
   D. Components of Linux
      1. Desktop
      2. Linux Commands
   E. System Tools
   F. Preferences and Settings
      1. Users
      2. Virtual Memory
   G. Maintenance
      1. Performance Monitoring
      2. Install and Uninstall Applications
      3. Apply System and Application Updates
      4. System Protection
II. System Implementation
   A. Processes and Procedures for Pre-Installation of the OS
   B. Installing of the OS
   C. Processes and Procedures for Post-Installation of the OS
III. Virtualization
   A. Components Included in Virtualization
      1. Physical Machine
      2. Hypervisor
      3. Virtual Machine
      4. Virtual Hard Disk (VHD)
   B. Types of Virtualization
      1. Full
      2. Partial
      3. Paravirtualization
   C. Security Benefits and Issues
IV. Disk Management
   A. Disk Types
      1. Dynamic vs. Basic
      2. Primary
4. Fruity
3. Extended
4. Logical
B. Disk Management
   1. Drive Status
   2. Adding Drives and Arrays
   3. Mounting, Extending, and Splitting
C. Optimization and Maintenance
   1. Disk Cleanup
   2. Check Disk
   3. Defrag
V. File Management
   A. File System Components
      1. Partition
      2. Volume
      3. Directory
      4. File
   B. File System Types
      1. FAT/FAT32
      2. New Technology File System (NTFS)
      3. Compact Disc File System (CDFS)
   C. Folder and File Management
      1. Common File Locations for Windows
      2. Common File Management Commands
   D. Sharing Folders and Files
      1. NTFS vs. Share Permissions
      2. File Attributes
      3. Cloud
VI. System Security
   A. Attack and Intrusion Methods and Countermeasures
      1. Social Engineering
      2. Malware
   B. Security Best Practices
      1. Principle of Least Privilege
      2. Account Management and Authentication
      3. Encryption
   C. Physical Security
      1. Building Security
      2. User Education
      3. Data Destruction
   D. Network Security
      1. Network Utilities
      2. Wired and Wireless Networks
      3. Firewalls
      4. Proxy Servers
VII. Mobile Devices
   A. Laptop vs. Mobile Device Features
   B. Operating Systems
   C. Network Connectivity
   D. System and Application Configuration
   E. Securing
VIII. Software Troubleshooting
   A. Operating System
   B. Windows Recovery
IX. PC Technician Role
A. Job-Related Professional Behavior
   1. Communication and Professionalism
   2. Private and Confidential Materials
   3. Customer Focus
B. Appropriate Tools to Ensure Safety
C. Computer Evidence Collection and Analysis
D. Appropriate Safety Procedures to Avoid Potential Hazards
   1. Electro-Static Discharge Precautions and Procedures
   2. Safe Work Environments
E. Disposal Procedures for Equipment and Hazardous Chemicals

MCCCD Governing Board Approval Date: December 13, 2016

All information published is subject to change without notice. Every effort has been made to ensure the accuracy of information presented, but based on the dynamic nature of the curricular process, course and program information is subject to change in order to reflect the most current information available.
Cisco Networking Basics

Course: CNT140  Lec + Lab  4 Credit(s)  6 Period(s)  5.4 Load
Course Type: Occupational
First Term: 2007 Fall  Load Formula: S
Final Term: 2017 Fall

Description: Introduction to the computer networking field. Covers network terminology and protocols, local area networks (LAN), and wide area networks (WAN). Includes Open Systems Interconnection (OSI) models, cabling and cabling tools, routers, router programming, Ethernet, Internet Protocol (IP) addressing, and network standards. Preparation for the Cisco Certified Network Associate examination.

Requisites: None

MCCCD Official Course Competencies

1. Explain physical connections of the computer to the Internet, connection testing, use of web browsers, and binary and hexadecimal numbers. (I)
2. Explain internetworking problems and solutions and their relationship to the seven layers of the Open Systems Interconnection (OSI) and the Transmission Control Protocol/Internet Protocol (TCP/IP) model. (II)
3. Describe the characteristics and types of cables and cabling specifications related to those devices. (III, IV)
4. Identify and describe the protocols, hardware, and cabling types related to local area networks (LANs) and wide area networks (WANs). (V)
5. Identify and describe Ethernet technology (VI, VII)
6. Identify and describe hardware devices used to work with broadcast and collision domains. (VI)
7. Explain concepts of binary and hexadecimal numbers and their conversion to and from decimal numbers. (VII)
8. Describe and demonstrate IP addressing and subnet masking, and explain how to obtain an Internet Protocol (IP) address. (VII, IX)
9. Contrast routed and routing protocols, and explain how subnetting relates to these practices. (VIII)
10. Describe and identify the protocols and technologies working at the Transport and Application layers of the Transmission Control/Internet Protocol TCP/IP model. (IX)

MCCCD Official Course Outline

I. Introduction to Networking
   A. Connecting to the Internet
   B. Network math
II. Networking Fundamentals
   A. Terminology
   B. Bandwidth
   C. Networking models
III. Networking Media

https://aztransmac2.asu.edu/cgi-bin/WebObjects/MCCCD.wa/va/freeForm2?id=50201
A. Copper media
B. Optical media
C. Wireless media

IV. Cable Testing
A. Frequency-based cable testing
B. Signals and noise
C. Methods of testing fiber optic cable
D. Attenuation and signal loss

V. Cabling LANS and WANS
A. Cabling the LAN
B. Cabling the WAN
C. Serial, integrated services digital network (ISDN) and digital subscriber lines (DSL) interfaces on routers

VI. Ethernet Fundamentals
A. Basic principles
B. Ethernet operation
C. 10-Mbps and 100-Mbps Ethernet
D. Gigabit and 10-Gigabit Ethernet
E. Ethernet switching
F. Collision and broadcast domains

VII. TCP/IP Protocol Suite and IP Addressing
A. Introduction to TCP/IP
B. Internet addresses
C. Obtaining an IP address

VIII. Routing Fundamentals and Subnets
A. Introduction to routers
B. Routed vs routing protocols
C. IP packet structure
D. Route tables and path determination
E. IP address classes and subnetting

IX. TCP/IP Transport and Application Layers
A. TCP/IP transport layer
B. Three-way handshake and windowing flow control
C. TCP vs user datagram protocol (UDP)
D. The application layer and its protocols

VI. Cisco Troubleshooting Procedures
A. Initial and subsequent testing
   1. Effects of EMI/RFI
   2. Causes of cross talk
B. Safe wiring systems
C. Solution strategies

MCCCD Governing Board Approval Date: 6/26/2007

All information published is subject to change without notice. Every effort has been made to ensure the accuracy of information presented, but based on the dynamic nature of the curricular process, course and program information is subject to change in order to reflect the most current information available.
Cisco - Routing and Switching Essentials

Course: CNT150AA
Lec + Lab 4.0 Credit(s) 6.0 Period(s) 6.0 Load
Course Type: Occupational
Load Formula: T
First Term: 2018 Fall
Final Term: Current

Description: Architecture, components, and operations of routers and switches in a small network. Students learn how to configure a router and a switch for basic functionality. Configuration and troubleshooting routers and switches and resolving common issues with RIPv1, RIPng, single-area and multi-area OSPF, virtual LANs, and inter-VLAN routing in both IPv4 and IPv6 networks. Preparation for Cisco certification examination.

Requisites: Prerequisites: A grade of C or better in CNT140AA or permission of Instructor.

MCCCD Official Course Competencies

1. Describe basic switching concepts and the operation of Cisco switches (I, II)
2. Describe the purpose, nature, and operations of a router, routing tables, and the route lookup process (IV, V, VI, VII)
3. Describe how VLANs create logically separate networks and how routing occurs between them (III, V)
4. Describe dynamic routing protocols, distance vector routing protocols, and link-state routing protocols (VII, VIII)
5. Configure and troubleshoot static routing and default routing (RIP and RIPng) (VI)
6. Configure and troubleshoot an Open Shortest Path First (OSPF) network (VIII)
7. Configure and troubleshoot access control lists (ACLs) for IPv4 and IPv6 networks (IX)
8. Configure and troubleshoot Dynamic Host Configuration Protocol (DHCP) for IPv4 and IPv6 networks (X)
9. Configure and troubleshoot Network Address Translation (NAT) operations (XI)

MCCCD Official Course Outline

I. Introduction to Switched Networks
   A. LAN Design
   B. The Switched Environment
II. Basic Switching Concepts and Configuration
    A. Basic Switch Configuration
    B. Switch Security: Management and Implementation
III. VLANs
    A. VLAN Segmentation
    B. VLAN Implementations
    C. VLAN Security and Design
IV. Routing Concepts
    A. Initial Configuration of a Router
    B. Routing Decisions
    C. Router Operation
V. Inter-VLAN Routing
    A. Inter-VLAN Routing Configuration
    B. Troubleshoot Inter-VLAN Routing

aztransmac2.asu.edu/cgi-bin/WebObjects/MCCCD.wca/wa/freeForm2?fid=129082
C. Layer 3 Switching

VI. Static Routing
A. Static Routing Implementation
B. Configure Static and Default Routes
C. Review of CIDR and VLSM
D. Configure Summary and Floating Static Routes
E. Troubleshoot Static and Default Route Issues

VII. Routing Dynamically
A. Dynamic Routing Protocols
B. Distance Vector Routing Protocols
C. RIP and RIPng Routing
D. Link-State Dynamic Routing
E. The Routing Table

VIII. Single-Area OSPF
A. Characteristics of OSPF
B. Configuring Single-Area OSPFv2
C. Configuring Single-Area OSPFv3

IX. Access Control Lists
A. IP ACL Operation
B. Standard IPv4 ACLs
C. Extended IPv4 ACLs
D. Troubleshoot ACLs
E. IPv6 ACLs

X. DHCP
A. Dynamic Host Configuration Protocol v4
B. Dynamic Host Configuration Protocol v6

XI. Network Address Translation for IPv4
A. NAT Operation
B. Configuring NAT
C. Troubleshooting NAT

MCCC D Program Description

MCCC D Governing Board Approval Date: June 24, 2014

All information published is subject to change without notice. Every effort has been made to ensure the accuracy of information presented, but based on the dynamic nature of the curricular process, course and program information is subject to change in order to reflect the most current information available.
Linux Operating System

Course: CIS126DL
First Term: 2018 Fall
Final Term: Current

Description: Introduction to the Linux Operating system. Develop knowledge and skills required to install, configure and troubleshoot a Linux-based workstation including basic network functions. Learn basic command line and Graphical User Interface (GUI) desktop environment utilities and applications. Fundamental abilities to achieve the entry-level industry certification covered.

Requisites: None

MCCCD Official Course Competencies

1. Understand the history and nature of Open Source software (I)
2. Demonstrate ability to install a variety of Linux distributions. (II)
3. Compare and contrast variety of Linux distributions (II)
4. Navigate the Linux file system hierarchy (II)
5. Create, manage, and delete user accounts, groups and permissions. (II)
6. Demonstrate basic Linux shell commands including file and directory commands, archiving and compression. (III)
7. Use the Visual Editor (VI) to edit and create text documents. (III)
8. Configure printers for use on a workstation or network. (IV)
9. Understand X Window system architecture. (IV)
10. Use graphic utility to configure graphic display. (IV)
11. Research shell commands using the 126help option and Manual (Man) pages. (V)
12. Install applications using Red Hat Package Manager (RPMs) and compression utilities such as Tape Archive (tar) and gzip. (V)
13. Use network-based applications such as browsers, telnet, file transfer protocol (FTP) and email. (V)
14. Demonstrate knowledge of a variety of GNU Object Model Environment (GNOME) and K Desktop Environment (KDE) applications. (V)
15. Troubleshoot problems related to operating system installation and configuration. (VI)

MCCCD Official Course Outline

I. Theory of Operation
   A. History of Open Source and Free Software
   B. How the Free Software Foundation’s (FSF) GNU (GNU’s Not Unix) Project lead to the General Public License (GPL)
   C. Third Party Analysis of Open Source Software
   D. Living with Free Software
   E. Linux System Concepts
F. Main Board Configuration Issues
G. Network Configuration

II. Base System
A. Installation Media
B. Component Compatibility and Configuration Responsibilities
C. Describe several Linux distributions and their tradeoffs
D. Installation of Linux
E. Compare and Contrast several Different Distributions of Linux
F. Start Up and Shut Down Sequences
G. File System Hierarchy
H. Basic System Navigation
I. Manage User Accounts

III. Shells and Commands
A. The Shell
B. Single character commands (interrupt, erase, etc.)
C. The ls command - directory listing
D. The cd command - change directory
E. More and less commands - pager utilities
F. The cp command - copy a file
G. The ln command - duplicate a directory or file
H. The mv command - move or rename a file
I. The mkdir command - make a directory
J. The rm command - remove a file
K. The rmdir command - remove a directory
L. The head and tail commands - peak at beginning or end of a file
M. The file command - view the file type
N. The grep command - search files for a target string
O. The du and df commands - show disk usage and free space
P. The tar command - places multiple files into one archive
Q. The gzip, gunzip, and zcat - un/compression utilities
R. The mtools - read and write MS-DOS files quickly
S. The find and locate - search for names in the file system
T. The Visual Editor (Vi) text editor

IV. System Services
A. Device Driver Utilities
B. Printer Configuration
C. The X Window System Architecture
D. Window Managers

V. Applications
A. Gathering Information
B. Network Applications including browser, email, telnet, secure shell, and file transfer
C. Text, Mark-up and Word Processing Programs
D. Office Applications
F. Graphics Applications

VI. Installation Troubleshooting
A. Linux Loader (LILO) and boot problems
B. Creation of rescue disks
C. Locked applications and processes
D. Printing errors
E. System logging
MCCCD Governing Board Approval Date: 12/9/2003

All information published is subject to change without notice. Every effort has been made to ensure the accuracy of information presented, but based on the dynamic nature of the curricular process, course and program information is subject to change in order to reflect the most current information available.
Linux System Administration

Course: CIS238DL  Lec + Lab  3.0 Credit(s)  4.0 Period(s)  4.0 Load
Course Type: Occupational
First Term: 2018 Fall  Load Formula: T
Final Term: Current

Description: Managing Linux Operating Systems including sophisticated manipulation of file structures, backup systems, printing processes, troubleshooting, user account management, hard disk maintenance and configuration, process monitoring and prioritizing, kernel customization, and system resource control. Preparation for industry certifications such as the CompTIA Linux+, the Red Hat Certified System Administrator (RHCSA), the Red Hat Certified Engineer (RHCE) and the Linux Professional Institute (LPIC-I).

Requisites: Prerequisites: A grade of C or better in CIS126DL or CIS126RH or permission of Instructor.

MCCCD Official Course Competencies

1. Demonstrate understanding of Linux File System standards. (I)
2. Demonstrate the utilization of automated backup procedures. (I, IV, V, VI)
3. Manage and control system resources such as memory and CPU usage through a variety of techniques. (I, IV, VI)
4. Configure printing system to local and remote network printers including print job filtering and management. (I, IV, VI)
5. Create and implement a security policy including an emergency security plan. (I, II, III, V, VI)
6. Design fault-tolerant systems and network environments. (I, V, VI)
7. Customize system security through the use of user system profiles, user and group accounts, and file and directory privileges. (II, III, V, VI)
8. Create partitions and file systems and manipulate access to them through the use of mount points and automated mounting techniques. (II, IV, VI)
9. Recompile the kernel of the Linux operating system from source code and explain the benefits. (II, III)
10. Apply su and sudo commands to access administrative system privileges. (III)
11. Monitor system functions and security through the use of a variety of system logs. (III)
12. Add to repertoire of system prompt commands used to control the Linux operating system. (I, II, III, IV, V, VI)
13. Apply a variety of command line and graphical applications to perform a variety of user and administrative tasks. (V)
14. Implement a variety of troubleshooting techniques to prevent and deal with a variety of system problems including core dumps. (VI)

MCCCD Official Course Outline

https://netaccess2.nmu.edu/npj-bin/WebObjects/MCCCD.wss/en/freeForm2?id=121894
I. Theory of Operation
   A. File system hierarchy standards
   B. Cron daemon’s (task scheduling utility) implementation of file system backup
   C. System tuning
   D. Print process and the role of the Berkeley Software Distribution (BSD) printing model
   E. Common physical network problems and the troubleshooting measures
   F. Emergency measures when network vulnerabilities are breached
   G. Key system resources
   H. Redundant Array of Independent Disks (RAID) storage

II. Base System
   A. Key files used in configuring user profiles
   B. Adding and removing users
   C. Run levels and specific roles of reserved run levels 0, 1, and 6
   D. File system table configuration file (fstab) in mounting and unmounting file systems and devices
   E. Recompiling the kernel

III. Shells and Commands
   A. Switch user (su) command
   B. Message of the day (motd) and its role in user communication
   C. Microsoft Disc Operating System OS (MS-DOS) tools and their use in a Linux system
   D. Make command in the compilation of source code
   E. Function of the touch command and its effect on system logs
   F. System status, system message logging, and performance analysis

IV. System Services
   A. Function of common user commands
   B. Utilities used for archiving
   C. File system check command (fsck) and program’s default run time
   D. Process management and the options that accompany those commands
   E. Printer configuration options
   F. Line printer daemon and the foreground line printer requester
   G. Package managers utilizing software packages

V. Applications
   A. Backup applications
   B. Mail exchange programs
   C. Web server daemons
   D. Processor, system architecture and compiler design
   E. File Transfer Protocol (FTP) clients and servers
   F. Secure Shell (SSH) network
   G. Common graphical configuration tools

VI. Troubleshooting
   A. Tools, procedures, and techniques for administering a variety of systems within the Linux architecture
   B. Measures to prevent and control core dumps
   C. Rescue environment utilities

MCCCD Governing Board Approval Date: November 28, 2017

All information published is subject to change without notice. Every effort has been made to ensure the accuracy of information presented, but based on the dynamic nature of the curricular process, course and program information is subject to change in order to reflect the most current information available.
Information Security Fundamentals

Course: ITS110
Lec + Lab 3.0 Credit(s) 4.0 Period(s) 4.0 Load
Course Type: Occupational
First Term: 2020 Fall
Load Formula: T - Lab Load
Final Term: Current

Description: Fundamental concepts of information technology security. Topics include authentication methods, access control, cryptography, Public Key Infrastructure (PKI), network attack and defense methods, hardening of operating systems and network devices, securing remote access and wireless technologies and securing infrastructures and topologies. Emphasis on hands-on labs in both the Windows and Linux environments. Builds on thorough understanding of Transmission Control Protocol/Internet Protocol (TCP/IP) and security concepts and Microsoft (MS) Windows and Linux Administration.

Requisites: Prerequisites: A grade of C or better in CIS126DL, or CIS126RH, or permission of Program Director. Corerequisites: BPC270 or MST150++.

MCCCD Official Course Competencies

1. Explain the need for authentication methods and available solutions. (I)
2. Implement appropriate access control methods and demonstrate techniques for monitoring access to network resources. (II)
3. Apply cryptographic methods to ensure data integrity and privacy. (III)
4. Explain the elements of Public Key Infrastructure and how to plan for implementation. (IV)
5. Identify the types of threats to networks and the steps to take to reduce these threats. (V)
6. Identify vulnerabilities in operating system software and network devices, and implement measures to mitigate these vulnerabilities. (VI)
7. Demonstrate methods to secure remote access to network resources. (VII)
8. Identify weaknesses in wireless technology and implement measures to secure wireless environments. (VIII)
9. Explain the methods used to design and maintain a secure network infrastructure. (IX)
10. Explain the techniques used to assess risk, detect network intrusions and ensure the continuity of network resources. (X)
11. Describe the elements of effective security policies in a business environment. (XI)

MCCCD Official Course Outline

I. Authentication methods
   A. Security terms
   B. Central Intelligence Agency and non-repudiation
   C. Security standards
   D. Kerberos
   E. Certificates
   F. Token-based authentication

https://maricopa.edu/og-and/WebObjects/MCCCD.wss/awt/seeForm?doc=145941
G. Challenge Handshake Authentication Protocol (CHAP)
H. Smart Cards
I. Biometrics
J. Extensible Authentication Protocol (EAP)

II. Access control
A. Access control terminology and concepts
B. Auditing and logging
C. Isolating the auditing system
D. Filtering logs
E. Audit trails and the collection of evidence
F. Access Control Methods Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role-Based Access Control (RBAC)
G. Balancing responsibilities of security

III. Cryptography
A. Cryptography and encryption
B. Common cryptography terms
C. Types of encryption algorithms
D. Services provided by encryption
E. Hash encryption
F. Symmetric-key encryption
G. Asymmetric-key encryption
H. Applied encryption

IV. Public Key Infrastructure (PKI)
A. PKI terms
B. Types of certificates
C. PKI standards and protocols
D. Public-Key Infrastructure X.509 (PKIX)
E. Certificate policies
F. Certificate Practice Statement (CPS)
G. Certificate revocation
H. Online Certificate Status Protocol (OCSP)
I. Trust models
J. Centralized and decentralized key management
K. Key management and certificate life cycles
L. Certificate and key storage
M. Planning for PKI

V. Network attacks and vulnerabilities
A. File Transfer Protocol/Internet Protocol (FTP/IP) protocol suite overview
B. Spoofing attacks
C. Scanning attacks
D. Denial-of-Service (DOS) attacks
E. Distributed Denial-of-Service (DDOS) attacks
F. Mitigating vulnerability and risk
G. Man-in-the-Middle attacks
H. Packet sniffing
I. TCP/IP Connection hijacking
J. Domain Name System (DNS) and Address Resolution Protocol (ARP) cache poisoning
K. Password-guessing attacks
L. Software exploitation
M. Back door
N. Weak keys
O. Birthday attack
P. Mathematical attacks
Q. Social Engineering
R. Hoaxes
S. Malicious code
T. Viruses
U. Worms
V. Illicit servers
W. Trojan horses and rootkits
X. Logic bombs
Y. Managing malware
Z. Auditing, logging and system scanning

VI. Operating system and application hardening
A. Security baselines
B. Client security issues
C. Encryption: Secure Socket Layer (SSL) and Transport Layer Security (TLS)
D. Isolating services and jails
E. Mail servers and Simple Mail Transport Protocol (SMTP) relay
F. File sharing
G. File transfer vulnerabilities
H. Server Message Block (SMB) encryption
I. File Transfer Protocol (FTP)
J. Securing web servers
K. DNS servers
L. Data repositories
M. Operating system hardening

VII. Securing remote access
A. Concepts, terminologies and methods
B. Virtual Private Networks (VPNs)
C. Terminal Access Controller Access Control System (TACACS and TACACS+)
D. Remote Authentication Dial-In User Service (RADIUS)
E. Internet Protocol Security (IPSec)
F. 802.1x
G. Remote administration methods
H. Secure Shell (SSH)

VIII. Wireless network security
A. Wireless technologies
B. Wireless networking modes
C. Wireless cells
D. Wireless Application Protocol (WAP)
E. Wireless Transport Layer Security (WTLS)
F. Wireless Vulnerabilities and Wired Equivalent Privacy (WEP)
G. Solutions for wireless network vulnerabilities
H. Site surveys and war driving

IX. Securing topologies and infrastructure
A. Firewall overview
B. Security topologies
C. Security zones
D. Virtual Local Area Network (LAN) (VLAN)
E. Network Address Translation (NAT)
F. Traffic control methods
G. Configuring firewalls
H. Configuring an Access Control List (ACL)
I. Network device hardening
J. Physical security
K. Cabling and network security
X. Risk analysis, intrusion detection and business continuity
   A. Risk identification
   B. Intrusion detection systems
   C. Honey pots
   D. Incident response policy
   E. Forensics
   F. Disaster recovery plan
   G. Business continuity
XI. Security policy management
   A. Security policy
   B. Human resource policies
   C. Documentation

MCCCD Governing Board Approval Date: February 25, 2020

All information published is subject to change without notice. Every effort has been made to ensure the accuracy of information presented, but based on the dynamic nature of the curricular process, course and program information is subject to change in order to reflect the most current information available.
Ethics in Information Technology

Course: CIS 111
Lecture 3 Credit(s) 3 Period(s) 3 Load
Course Type: Occupational
Load Formula: S - Standard

First Term: 2014 Fall
Final Term: Current

Description: Ethical issues that arise as a result of increasing use of computers, and the responsibilities of those who work with computers, either as computer science professionals or end users. Critical inquiry and review of ethical challenges in information technology business, including professional and corporate responsibility, government regulation, fiduciary responsibilities of information, infringement of intellectual property, security risk assessment, Internet crime, identity theft, employee surveillance, privacy, compliance, social networking, and the ethics of IT corporations.

Requisites: Prerequisites: None.

MCCCD Official Course Competencies

1. Describe a variety of different ethical theories. (I)
2. Describe professional business ethics and the complexities of making ethical judgments. (I)
3. Describe issues relating to corporate ownership, corporate governance, and responsiveness to corporate stakeholders. (II)
4. Explain how social media responsibility encompasses economic, legal, ethical, and privacy issues. (II)
5. Explain whistle-blowing and protection for whistle-blowers. (II)
6. Describe the major ethical challenges of operating in a healthcare environment using mobile and wireless technologies. (II)
7. Explain fiduciary responsibilities of private information. (II)
8. Describe issues with software and software liability. (III)
9. Explain cost/benefit analysis in information technology ethical decision-making. (III)
10. Describe the influence of government regulations as well as professional self-regulation and sanctions in ethical information technology decision-making. (IV)
11. Explain intellectual property, copyright laws, and fair use doctrine. (IV)
12. Define hate speech and defamation. (V)
13. Review contemporary issues related to workplace monitoring. (V)
14. Describe the major identity theft issues. (V)
15. Describe Information Technology security breaches and risk assessments. (V)
16. Define security policies within Information Technology. (V)
17. Describe professional codes of ethics for Information Technology professionals. (V)
18. Describe prevention, detection, and responses to Information Technology security attacks. (V)

MCCCD Official Course Outline

I. Ethics and Ethical Theories
   A. Sources of ethical theories

https://arizona.mcccd.edu/learning/Weblinks/MCCCD.wss/ea/teacourse2?id=74479
B. Definition of professional Information Technology ethics
C. Application of ethical theories to business

II. Corporate and Individual Responsibilities
A. Responsibilities to shareholders
B. Responsibilities to stakeholders
C. Social media responsibility
D. Healthcare information privacy issues with mobile and wireless technologies
E. Fiduciary responsibilities concerning private information
F. Whistle-blower rights and responsibilities

III. Obligations in the Information Technology Profession
A. Describe liabilities related to software
B. Give examples of secure coding
C. Give examples of cost/benefit analysis in information technology ethical decision-making

IV. Decision-Making in Information Technology
A. Describe the influence of government regulations and professional self-regulation The professional and corporate social audit
B. Describe intellectual property, copyright laws, and fair use doctrine

V. Application of Ethics to Specific Areas of Information Technology
A. Explain hate speech and defamation
B. Explain privacy issues related to workplace monitoring
C. Give examples of Information Technology security breaches and risk assessments
D. Define security policies within Information Technology
E. Describe prevention, detection, and responses to Information Technology security attacks
F. Describe the major identity theft issues
G. Describe the professional code of ethics for Information Technology professionals

MCCCD Governing Board Approval Date: June 24, 2014

All information published is subject to change without notice. Every effort has been made to ensure the accuracy of information presented, but based on the dynamic nature of the curricular process, course and program information is subject to change in order to reflect the most current information available.
Python Programming: Level I

Course: CIS156  Lec + Lab 3.0 Credit(s) 4.0 Period(s) 4.0 Load
Course Type: Occupational
First Term: 2021 Fall  Load Formula: T : Lab Load
Final Term: Current

Description: Introduction to Python programming. Includes general concepts, program design, development, data types, operators, expressions, flow control, functions, classes, input and output operations, debugging, structured programming, and object-oriented programming.

Requisites: Prerequisites: A grade of C or better in CIS105 or permission of Instructor.

MCCCD Official Course Competencies

1. Explain the development of Python applications. (I)
2. Explain the control structures in Python. (II)
3. Utilize basic data structures in Python. (III, IV)
4. Utilize string and character manipulation in Python. (V)
5. Utilize object-oriented programming concepts in Python. (VI)
6. Utilize Python to load, save and manipulate persistent data. (VII)
7. Identify and debug common mistakes in programs written in Python. (VIII, IX)

MCCCD Official Course Outline

I. Python language
   A. History of Python
   B. Operators
   C. Variables
   D. Terminology
   E. Selection structure
II. Control structures/statements
   A. Counter-controlled repetition
   B. For repetition
   C. While repetition
   D. Break and Continue statements
III. Functions
   A. Program functions in Python
   B. Class methods
   C. Using Python modules
   D. Recursion vs. Iteration
IV. Data structures operations
   A. Lists
   B. Tuples
   C. Dictionaries

https://masonite2.xrs.edu/g-bim/WebObjects/MCCCD.wss/eu/fmeForm1?id=163971

1/2
V. String and characters
   A. Fundamentals of characters and strings
   B. String constructors
   C. Concatenating strings
   D. String methods

VI. Object-oriented programming
   A. Definition
   B. Class scope and access
   C. Constructors /Methods
   D. Abstraction
   E. Software reusability
   F. Encapsulation
   G. Inheritance
   H. Composition

VII. Data persistence
   A. Read and write text data to text files
   B. Support of database connectivity
   C. Issue embedded SQL commands (SELECT/UPDATE/INSERT/DELETE) via Python

VIII. Debugging
   A. Syntax errors
   B. Logic errors
   C. Run-time errors
   D. Debugging techniques
   E. Test data

IX. Exception handling
   A. The basics of Python error-handling
   B. Error-handling techniques
   C. Try blocks
   D. Throwing, catching, and re-throwing an exception

MCCCD Governing Board Approval Date: February 23, 2021

All information published is subject to change without notice. Every effort has been made to ensure the accuracy of information presented, but based on the dynamic nature of the curricular process, course and program information is subject to change in order to reflect the most current information available.
Chandler Technical Center
ICON Setup

Year One cybersecurity setup for Chandler Technical Center. Year One classes include:
- Intro to Computer Systems
- Hardware and Software (A & B)

Intro to Computer Systems
- MS Office Apps
- Internet access
- eBook curriculum

Hardware / Software Lab Setup
- Lab Tables w/integrated power (like we have @ BHS)
- Anti-Static Mat on the tables
- eBook curriculum
- Packet Tracer software

Computer Kit – the kit requirements will vary upon how you choose to allow students to connect for the purpose of downloading OS and various drivers (PacketTracer is now on the approved software list)

<table>
<thead>
<tr>
<th>Component</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>9. Motherboard – ATX (full size)</td>
<td>31</td>
</tr>
<tr>
<td>a. LGA1200 – Intel</td>
<td></td>
</tr>
<tr>
<td>10. CPU w/heat sink &amp; fan</td>
<td>31</td>
</tr>
<tr>
<td>11. Graphics Processing Card</td>
<td>31</td>
</tr>
<tr>
<td>12. RAM (8GB) - recommended by Cisco (2 X 4GB suggested) needed for VM practice in curriculum</td>
<td>31</td>
</tr>
<tr>
<td>13. Case (ATX)</td>
<td>31</td>
</tr>
<tr>
<td>14. Ethernet Card</td>
<td>31</td>
</tr>
<tr>
<td>15. PCI / PCIe</td>
<td>31</td>
</tr>
</tbody>
</table>

This storage setup will allow students to configure their machine and NOT have to reverse all their work for the next class. Each student would be assigned an SSD that would remain in the classroom and used for their work in the lab

<table>
<thead>
<tr>
<th>Component</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>16. Storage</td>
<td>31 Bays</td>
</tr>
<tr>
<td>a. Swappable SSD</td>
<td>1/Tray per SSD</td>
</tr>
<tr>
<td>i. Bay (30) - ~$25/ea (CDW)</td>
<td></td>
</tr>
<tr>
<td>ii. Trays (1 for each student) - ~$11/ea (CDW)</td>
<td>1/per student</td>
</tr>
<tr>
<td>b. SSD – 120GB (1 for each student) - ~$30/ea (CDW)</td>
<td></td>
</tr>
</tbody>
</table>
Cables
- Ethernet UTP bulk cable (CAT5e)
- Stranded UTP bulk cable (CAT5e)
- RJ45 connectors – Stranded and Solid Core
- RJ45 Network Cable Tester
- Crimpers
- Multimeter
- Networking scissors
- Cable stripper
- PC Power Supply Tester
- Anti-Static Duster
- Network Cable Tester

Tools
- 11-piece PC computer tool kit
- Anti-static wrist strap

Printer
Switch / Router
HDMI Monitors

ULINE Search Results: Stainless Steel Mobile Security Cage
# Chandler HS Lab Tool Proposal

<table>
<thead>
<tr>
<th>Item</th>
<th>Qty</th>
<th>Vendor</th>
<th>Picture</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Multimeter, MSR-C600</td>
<td>2</td>
<td>Amazon</td>
<td><img src="image" alt="Digital Multimeter" /></td>
<td>$49.98</td>
</tr>
<tr>
<td>PC Power Supply Tester</td>
<td>2</td>
<td>Amazon</td>
<td><img src="image" alt="PC Power Supply Tester" /></td>
<td>$36.38</td>
</tr>
<tr>
<td>11 Piece PC Computer Tool Kit</td>
<td>31</td>
<td>Amazon</td>
<td><img src="image" alt="11 Piece PC Computer Tool Kit" /></td>
<td>$827.08</td>
</tr>
<tr>
<td>Anti-Static Wrist Strap</td>
<td>5</td>
<td>Amazon</td>
<td><img src="image" alt="Anti-Static Wrist Strap" /></td>
<td>$59.95</td>
</tr>
<tr>
<td>MetroVac Anti-Static Electric Duster</td>
<td>2</td>
<td>Amazon</td>
<td><img src="image" alt="MetroVac Anti-Static Electric Duster" /></td>
<td>$259.98</td>
</tr>
<tr>
<td>Cable Crimpers RJ45 Crimp</td>
<td>30</td>
<td>Amazon</td>
<td><img src="image" alt="Cable Crimpers RJ45 Crimp" /></td>
<td>$419.70</td>
</tr>
<tr>
<td>RJ45 Connectors SHD CAT6 Solid/Stranded Core</td>
<td>10</td>
<td>Amazon</td>
<td><img src="image" alt="RJ45 Connectors SHD CAT6 Solid/Stranded Core" /></td>
<td>$144.90</td>
</tr>
<tr>
<td>Item Description</td>
<td>Quantity</td>
<td>Supplier</td>
<td>Price</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>NavePoint CAT5e, Solid Bulk Ethernet Cable UTP</td>
<td>1</td>
<td>Amazon</td>
<td>$56.42</td>
<td></td>
</tr>
<tr>
<td>Belkin 250 ft CAT5e Stranded UTP Bulk Networking Cable</td>
<td>1</td>
<td>Amazon</td>
<td>$63.03</td>
<td></td>
</tr>
<tr>
<td>RJ45 Network Cable Tester for LAN Phone/RJ45 WireTestTool</td>
<td>30</td>
<td>Amazon</td>
<td>$299.70</td>
<td></td>
</tr>
<tr>
<td>Networking Scissors</td>
<td>5</td>
<td>Amazon</td>
<td>$99.85</td>
<td></td>
</tr>
<tr>
<td>Network Cable Tester</td>
<td>1</td>
<td>Amazon</td>
<td>$22</td>
<td></td>
</tr>
<tr>
<td>Mini Wire Stripper</td>
<td>1</td>
<td>Amazon</td>
<td>$8</td>
<td></td>
</tr>
<tr>
<td><strong>Total Cost</strong></td>
<td></td>
<td></td>
<td>$2,346.97</td>
<td></td>
</tr>
</tbody>
</table>
Arizona Department of Education CTE Recommended Equipment List

## Network Security

### Recommended Equipment and Software

<table>
<thead>
<tr>
<th>Item</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cable Cutter, Coax</td>
<td>30</td>
</tr>
<tr>
<td>Crimp Tool W/ Stripper, RJ11, RJ45</td>
<td></td>
</tr>
<tr>
<td>File, Flat Needle</td>
<td></td>
</tr>
<tr>
<td>Flashlight, Tactical L.E.D.</td>
<td>5</td>
</tr>
<tr>
<td>Forceps, Straight w/Grip</td>
<td></td>
</tr>
<tr>
<td>Handle, For Blades, Drive-Loc</td>
<td>2</td>
</tr>
<tr>
<td>Hex Keys Set, Fold-Up .050&quot; to 3/16&quot;</td>
<td></td>
</tr>
<tr>
<td>Insertion/Extraction Tool</td>
<td></td>
</tr>
<tr>
<td>Nutdriver Blade, 3/16&quot; 1/4, 5/16, 3/8</td>
<td></td>
</tr>
<tr>
<td>Pliers, Diagonal 4&quot; W/Spring</td>
<td></td>
</tr>
<tr>
<td>Pliers, Long Nose 4 3/4&quot;, 6&quot; w cutter</td>
<td></td>
</tr>
<tr>
<td>Pliers, Slip Joint 6&quot;</td>
<td></td>
</tr>
<tr>
<td>Pliers, Vise-Grip Long Nose 6&quot;</td>
<td></td>
</tr>
<tr>
<td>Punchdown Tool W/110 Blade</td>
<td>5</td>
</tr>
<tr>
<td>Receptacle Analyzer</td>
<td></td>
</tr>
<tr>
<td>Screwdriver, Phillips #0 x 2&quot;, 1x3, 2x4</td>
<td>30</td>
</tr>
<tr>
<td>Screwdriver, Slot 1/4&quot; x 6&quot;</td>
<td></td>
</tr>
<tr>
<td>Screwdriver, Slot 3/16&quot; x 4&quot;</td>
<td></td>
</tr>
<tr>
<td>Screwdriver, Slot 3/32&quot; x 2&quot;</td>
<td></td>
</tr>
<tr>
<td>Screwdriver, Stubby 2 in 1</td>
<td></td>
</tr>
<tr>
<td>Soldering Iron, 25 Watt 3-wire</td>
<td>3</td>
</tr>
<tr>
<td>Telephone Line Tester</td>
<td></td>
</tr>
<tr>
<td>Tone Line Aid W/Volume Control (Multimeters)</td>
<td></td>
</tr>
<tr>
<td>Tone Tracer, High Powered (Circuit Testers)</td>
<td></td>
</tr>
<tr>
<td>Trimpot Tool</td>
<td></td>
</tr>
<tr>
<td>Wire Strippers, &quot;T&quot; 16-28, (1)</td>
<td></td>
</tr>
<tr>
<td>Wrench, Adjustable 6&quot; Ergonomic</td>
<td>31</td>
</tr>
<tr>
<td>Desktops/ Laptops/ or I-pads</td>
<td>12</td>
</tr>
<tr>
<td>Routers</td>
<td>12</td>
</tr>
<tr>
<td>Servers</td>
<td>2</td>
</tr>
<tr>
<td>Switches</td>
<td>12</td>
</tr>
<tr>
<td><strong>Software tools for Analysis</strong></td>
<td></td>
</tr>
<tr>
<td>Network protocol analyzer, e.g. TShark, iPerf3 to support tuning of many parameters buffers, and protocols (TCP, UDP, SCTP with IPv4 and IPv6)</td>
<td>Wireshark and Packet Tracer</td>
</tr>
<tr>
<td>Security scanner to create a map of the network</td>
<td></td>
</tr>
<tr>
<td>Debugger program to find communication and/or data problems in SNMP monitoring configurations</td>
<td></td>
</tr>
<tr>
<td>IP address and port scanner</td>
<td></td>
</tr>
<tr>
<td>IP calculator</td>
<td></td>
</tr>
</tbody>
</table>

Arizona Department of Education CTE Recommended Equipment List  1 of 2  Career and Technical Education  Network Security  6/16/2021
<table>
<thead>
<tr>
<th>Monitoring &amp; Logging</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Network monitoring software solution to dig deep into the health and integrity of your systems and network. An approach to monitoring.</td>
<td></td>
</tr>
<tr>
<td>system usage software.</td>
<td></td>
</tr>
<tr>
<td>NetFlow Analyzer</td>
<td>Red Hat, Ubuntu, MS Server, AWS Cloud, VMWare</td>
</tr>
<tr>
<td>Server software</td>
<td></td>
</tr>
<tr>
<td>Configuration &amp; Transfer software</td>
<td>Clonezilla, Tera Term, puTTY, UDP Cast</td>
</tr>
<tr>
<td>a multi-vendor Python library</td>
<td>Internet access to IP &amp; PMP Modules</td>
</tr>
<tr>
<td>network device software.</td>
<td></td>
</tr>
<tr>
<td>Platform supports</td>
<td>Operating system keys for each student</td>
</tr>
<tr>
<td>TFTP Server</td>
<td>Can be installed on server software</td>
</tr>
<tr>
<td>SFTP/SCP Server software</td>
<td>Can be installed on server software</td>
</tr>
</tbody>
</table>

For Network troubleshooting: https://www.pluralsight.com/blog/it-ops/network-troubleshooting-tools

Free tools: https://www.networkmanagementsoftware.com/top-17-free-tools-for-network-administrators/

Sensors: pressure, magnetic, resistive, capacitance, photo electric

PLC's
Motors
Actuators
relays
IC controllers
Breadboard
switches
Printed circuit boards PCBs
Power supplies

Programmable manipulators
1 cartesian
(2) gantry
(3) cylindrical
(4) spherical
(5) articulated
(6) SCARA

Robot controls
1 Point to point (PTP)
2 Continuous Path control
3 Controlled path control

Automation and programming control tools
Programmable Computer Numeric control
Direct Numeric Control DNC
Printed Circuit Boards (PCB's)
computer-integrated manufacturing (CIM)
HMI software
PAC, PLC and controllers software

*Must meet the guidelines for specialized computing equipment as outlined on the "CTE Equipment Guidelines" at www.azed.gov/cte/grants

<table>
<thead>
<tr>
<th>Additional Items:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Scissors:</td>
<td>10</td>
</tr>
<tr>
<td>CAT6 Cable:</td>
<td>500ft</td>
</tr>
<tr>
<td>RF45 Connectors:</td>
<td>1000</td>
</tr>
<tr>
<td>Network Patch Panel:</td>
<td>4</td>
</tr>
<tr>
<td>Anti-Static Electric Duster:</td>
<td>2</td>
</tr>
<tr>
<td>Anti-Static Wrist Strap:</td>
<td>30</td>
</tr>
<tr>
<td>PC Computer Tool Kit:</td>
<td>30</td>
</tr>
<tr>
<td>Digital Multimeter:</td>
<td>2</td>
</tr>
<tr>
<td>Computer Kit:</td>
<td>31</td>
</tr>
<tr>
<td>RAM:</td>
<td>31</td>
</tr>
</tbody>
</table>

Arizona Department of Education
Career and Technical Education
Recommended Equipment List: Network Security

2 of 2
6/16/2021
# Appendix L: Cybersecurity Program Partnership Pathway

## Basha High School – Cyber Academy

- **CIS105**: Survey of Computer Information Systems 3 Credits
- **BPC270**: A+ Exam Prep: Operating System Configuration 3 Credits
- **CIS1250L OR CIS126RH**: Linux Operating System OR Red Hat System Administration I 3 Credits
- **CNT140AB**: Introduction to Networks (Cisco) 4 Credits
- **CNT150**: Routing and Switching Essentials (Cisco) (added to BHS part of cyber path w/CGCC) 4 Credits
- **CIS338L OR CIS338RH**: System Administration OR Red Hat System Administration II 3 Credits
- **ITS110**: Information Security Fundamentals 3 Credits
- **CIS155**: Python Programming 3 Credits
- **CIS111**: Ethics in Information Technology 3 Credits

## Chandler-Gilbert Community College

- **ITS240**: Ethical Hacking & Network Defense 3 Credits
- **CIS290AC OR CIS298AC**: Computer Information Systems Internship OR Special Projects 3 Credits
- **ITS291**: Computer Forensics Foundations 4 Credits
- **ITS292**: Advanced Computer Forensics 4 Credits
- **ENG101**: First Year Composition 3 Credits
- **ENG102**: First Year Composition 3 Credits
- **CRE101 or test exempt**: College Critical & Evaluative Reading or Exemption by Assessment if exempt, must substitute with Literacy [L] course 3 Credits
- **MAT141/142**: College Mathematics 3-4 Credits
- **COM 100, 110, or 230** (COM 100, 110, or 230 will count as SB course for UA credit) 3 Credits
- **HU**: Any approved Humanities, Arts, & Design course 3 Credits
- **SB**: Any approved Social- Behavioral Sciences course 3 Credits
- **SQ**: Any approved Natural Science course 4 Credits

## Additional BAS Requirements

- **HU**: Any approved Humanities, Arts, & Design course 3 Credits
- **LANG**: Second Language Proficiency (second semester level proficiency) 0-8 Credits

## University of Arizona - Chandler

- **ENGR 306**: Advanced Composition 3 Credits
- **BASV 314**: Mathematics for Applied Science 3 Credits
- **APCS 320**: Computational Thinking & Doing 3 Credits
- **CYSV 326**: Introductory Methods of Network Analysis 3 Credits
- **CYSV 379**: Cyber Ethics 3 Credits
- **CYSV 385**: Introduction to Cyber Operations 3 Credits
- **CYSV 400**: Active Cyber Defense 3 Credits

---

*08/03/2021*
<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBV 388</td>
<td>Cyber Investigations and Forensics</td>
<td>3</td>
</tr>
<tr>
<td>CYBV 435</td>
<td>Cyber Threat Intelligence</td>
<td>3</td>
</tr>
<tr>
<td>CYBV 473</td>
<td>Violent Python</td>
<td>3</td>
</tr>
<tr>
<td>CYBV 480</td>
<td>Cyber Warfare</td>
<td>3</td>
</tr>
<tr>
<td>CYBV 488</td>
<td>Senior Capstone</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Defense/Forensics Electives (choose 1 course)</td>
<td></td>
</tr>
<tr>
<td>CYBV 436</td>
<td>Counter Cyber Threat Intelligence</td>
<td>3</td>
</tr>
<tr>
<td>CYBV 454</td>
<td>Malware Threats &amp; Analysis</td>
<td>3</td>
</tr>
<tr>
<td>CYBV 471</td>
<td>Assembly Language Programming for Security Professionals</td>
<td>3</td>
</tr>
<tr>
<td>CYBV/NETV477</td>
<td>Advanced Cyber Forensics</td>
<td>3</td>
</tr>
<tr>
<td>CYBV 481</td>
<td>Social Engineering</td>
<td>3</td>
</tr>
</tbody>
</table>
Appendix M: Network Security Technical Standards 11.1999.00

An Industry Technical Standards Validation Committee developed and validated these standards on January 31, 2019. The Arizona Career and Technical Education Quality Commission, the validating authority for the Arizona Skills Standards Assessment System, endorsed these standards on July 14, 2019.

Note: Arizona’s Professional Skills are taught as an integral part of the Network Security program.

The Technical Skills Assessment for Network Security is available SY2020-2021.

Note: In this document i.e. explains or clarifies the content and e.g. provides examples of the content that must be taught.

STANDARD 1.0 APPLY PROBLEM-SOLVING AND CRITICAL THINKING SKILLS TO NETWORK SECURITY

1.1 Describe methods to determine priorities in establishing and maintaining a computer network
1.2 Prepare a plan of work and schedule network technology tasks
1.3 Apply problem-solving processes to network technology tasks (i.e., bottom-up, divide-and-conquer, top-down, etc.)
1.4 Prepare and present technical information for nontechnical and technical audiences in writing and verbally

STANDARD 2.0 MAINTAIN A SAFE AND ENVIRONMENTALLY CONSCIOUS WORK ENVIRONMENT

2.1 Identify personal responsibility for developing and maintaining a safe and healthy work environment
2.2 Use equipment, materials, and tools commonly used in the field of network security correctly and safely
2.3 Identify ergonomic solutions to prevent injuries common to network security tasks
2.4 Determine safe working practices to avoid or eliminate electrical hazards and physical injuries
2.5 Identify techniques used to manage power consumption in the networked environment (i.e., cloud-based, software defined, etc.)
2.6 Explain environmental considerations when disposing of computer/network components
2.7 Describe and resolve most common electrostatic discharge (ESD) hazards in a network environment

STANDARD 3.0 SPECIFY NETWORK SECURITY BEST PRACTICES, RISKS, AND THREATS

3.1 Perform risk management activities (e.g., define risk, determine risk level, and identify methods to address risk)
3.2 Define policies to manage system and data availability, confidentiality, and integrity
3.3 Classify data according to its sensitivity and criticality (i.e., mission critical, protect cafeteria menu vs. personal, financial and health information, trade secrets, etc.)
3.4 Identify security threats related to computer data, hardware, and software (i.e., denial of service, eavesdropping, intrusion, unauthorized access, unauthorized use, etc.)
3.5 Explain the importance of physical security of computer and network hardware following best practices (i.e., cameras, locks, USB port blocking, etc.)
3.6 Describe network threats (i.e., denial of service, email spoofing, hacking/cracking, intrusion, malware, phishing, social engineering, spamming, system vulnerabilities, website defacement, etc.)
3.7 Describe best practices to protect against network threats (i.e., access control, antivirus software, awareness and training, encryption, firewalls, incident detection systems/tools, intrusion detection prevention, network segmentation, port/service blocking, software updates/patches, etc.)
3.8 Define best practices to protect data at rest, data in transit, and data during processing
3.9 Describe password best practices (i.e., age, complexity, history, length, lockout, etc.)
3.10 Analyze authentication methods used to secure access to the network [i.e., biometrics, key cards, multi-factor authentication (MFA), passwords, single sign-on (SSO), two-factor authentication (2FA), etc.]
3.11 Identify best practices for access control (i.e., changing default passwords, disabling unused accounts, least privileges, privileged account management, role-based access control, etc.)

STANDARD 4.0 INVESTIGATE LEGAL AND ETHICAL ISSUES RELATED TO NETWORK SECURITY
4.1 Explore issues regarding intellectual property rights including software licensing and software duplication [i.e., Business Software Alliance, Creative Commons, Digital Right Management (DRM), https://www.ip-watch.org/about/, https://www.eff.org/, etc.]
4.2 Differentiate among freeware, open source, proprietary, and shareware software relative to legal and ethical issues
4.3 Identify issues, laws, and trends affecting data and privacy [e.g., Certified Network Professional (CNP), General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), and Sarbanes-Oxley Act (SOX)]
4.4 Describe acceptable use of industry-related data, private and public networks, and social networking

STANDARD 5.0 DEMONSTRATE BASIC COMPUTER MATHEMATICS REQUIRED FOR NETWORK SECURITY
5.1 Explain the function of base number systems in mathematics as it relates to network technology
5.2 Perform decimal to binary and binary to decimal conversions
5.3 Perform decimal to hexadecimal and hexadecimal to decimal conversions
5.4 Perform hexadecimal to binary and binary to hexadecimal conversions
5.5 Determine the appropriate method to perform conversions (e.g., paper-pencil and electronic resources)
5.6 Apply basic Boolean logic for actions such as Google searches and scripting (e.g., “and,” “nor,” “not,” and “or”)

STANDARD 6.0 DESCRIBE THE DEVELOPMENT AND EVOLUTION OF COMPUTERS AND NETWORK SECURITY
6.1 Describe a computer and its components and functions
6.2 Explain the historical evolution of the computer and computer networks
6.3 Explain how the development of computers has impacted modern life
6.4 Identify the components and structure of an information system [e.g., applications, media (cables, fiber, and wireless), network devices (router, switches, etc.), operating systems, and servers]
6.5 Discuss future trends and societal impacts in digital devices and network technology [i.e., Internet of Things (IoT), privacy, etc.]

STANDARD 7.0 DEMONSTRATE NETWORK MEDIA AND TOPOLOGIES
7.1 Specify the characteristics and main features of various networking topologies (e.g., bus, mesh, ring, and star)
7.2 Compare proper physical network topology
7.3 Identify appropriate connectors, media types, and uses for various networks
7.4 Compare physical and virtual networks [i.e., Software-Defined Wide-Area Network (SD-WAN), Virtual Local Area Network (VLAN), etc.]
7.5 Specify the characteristics of physical network technologies including cable types, length, speed, and topology
7.6 Specify the characteristics of wireless network technologies including frequency, speed, topology, and transmission (i.e., local area, metropolitan area, wide area networks, etc.)
7.7 Describe the structure of the internet (network of networks)
7.8 Identify the features, functions, and purpose of commonly used network components [i.e., routers, modem, switches, bridges, hubs, NIC (network interface card), etc.]
STANDARD 8.0 DESCRIBE NETWORK PROTOCOLS AND STANDARDS

8.1 Describe the parts and use of a Media Access Control (MAC) address
8.2 Describe the characteristics, name, and use of the seven layers of the Open Systems Interconnect (OSI) model
8.3 Describe the characteristics, name, and use of the four layers of the Transmission Control Protocol/Internet Protocol (TCP/IP) model
8.4 Explain the purpose of dynamic and static routing protocols
8.5 Explain the concept of ports and identify the three port ranges used in networking services and protocols [i.e., dynamic/private (49152-65535), system (0-1023), user (1024-49151), etc.]
8.6 Describe standard network ports and protocols [e.g., Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), Point-of-Presence (POP), Simple Mail Transfer Protocol (SMTP), etc.]
8.7 Describe the applications and characteristics of Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)
8.8 Differentiate IPv4/IPv6 addresses and their corresponding subnet masks [i.e., classful networks, Classless Interdomain Routing (CIDR), private vs public IP]
8.9 Summarize the basic characteristics and protocols of Metropolitan Area Network (MAN), Software-Defined Wide Area Network (SD-WAN), and Wide Area Network (WAN) technologies [i.e., Asynchronous Transfer Mode (ATM), frame relay, Multiprotocol Label Switching (MPLS), etc.]
8.10 Describe remote access protocols and services
8.11 Describe the function and purpose of security protocols [i.e., Hypertext Transfer Protocol Secure (HTTPS), Secure File Transfer Protocol (SFTP), tunneling, Virtual Private Network (VPN), etc.]
8.12 Explain the importance of proper documentation in accordance with industry standards

STANDARD 9.0 CONFIGURE A BASIC NETWORK

9.1 Design a network map with virtual and physical segments
9.2 Construct dynamic and static routes
9.3 Explain proper labeling in accordance with industry standards (i.e., cable, device, rack, wall plates, etc.)
9.4 Describe the components needed and purpose to build fault tolerance into a network
9.5 Describe the purpose of a disaster recovery plan for a network
9.6 Install and configure a physical and/or virtual networked system (i.e., Linux/UNIX, Windows, etc.)
9.7 Configure network cards, network settings, and operating system
9.8 Configure and connect devices to the network (i.e., computers, printers, routers, switches, etc.)
9.9 Identify the appropriate tools to use for diagnostic tasks or network repair (i.e., execute Traceroute, ipconfig, Ping, etc.)

STANDARD 10.0 HARDEN A NETWORK

10.1 Identify common network threats (i.e., denial of service, eavesdropping, intrusion, probing, unauthorized access, etc.)
10.2 Identify physical network threats [i.e., disrupting media (like cutting fiber), environmental/power disruption, unauthorized access to devices, etc.]
10.3 Describe the benefits and purpose of segmenting networks
10.4 Describe the benefits of disabling ports and network services
10.5 Describe the techniques to secure a Wi-Fi network [i.e., Extensible Authentication Protocol (EAP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2), etc.]
10.6 Compare the various types of firewalls and their uses (i.e., application, packet filtering, stateful, etc.)
10.7 Describe the benefits, disadvantages, and purpose of using a proxy service
10.8 Describe the benefits, disadvantages, and purpose of using network intrusion detection/prevention systems [i.e., Intrusion Detection System / Intrusion Prevention System (IDS/IPS), etc.]
10.9 Modify an existing network diagram with appropriate network hardening devices or systems
STANDARD 11.0 PERFORM NETWORK MAINTENANCE AND RESOLVE ISSUES

11.1 Identify maintenance tasks and create a schedule

11.2 Describe the purpose and benefits of network utilities [i.e., Network Statistics (Netstat), Name Server Lookup (NsLookup), Ping, Traceroute, etc.]

11.3 Demonstrate the use of visual indicators (i.e., indicator lights on devices, etc.) and diagnostic utilities (i.e., Wireshark, etc.) to interpret problems

11.4 Identify connectivity issues in various node environments (i.e., smart phones, switches, tablets, Linux/UNIX, Windows, etc.)

11.5 Identify and resolve network issues (i.e., cable failure, connection failure, environmental, misconfigurations, power, user error, etc.)

11.6 Identify common tools and methods of monitoring a network
Appendix N: Network Security 11.199.00 Program Description

NETWORK SECURITY 11.199.00
Program Description, Industry Credential, Coherent Sequence, and Teacher Certification

PROGRAM DESCRIPTION
The Network Security instructional program prepares students to assess the security needs of computer and network systems, recommend safeguard solutions, and manage the implementation and maintenance of security devices, systems, and procedures. Students who successfully complete the Network Security program’s coherent sequence of instruction will develop skill to analyze, test, troubleshoot, and evaluate existing network systems, such as local area network (LAN), wide area network (WAN), and Internet systems or a segment of a network system.

Perform network maintenance to ensure networks operate correctly with minimal interruption. Throughout the Network Security instructional program, students will enhance their technical knowledge and skills that are associated with functions of application integrity, cyber threat management, and infrastructure security within Network Technologies’ occupations. In addition to the occupation-related skills, students completing this program will also develop advanced critical thinking and applied academic foundational skills.

The Network Security Career and Technical Education program is delivered as a coherent sequence of courses designed to offer students’ knowledge and skills that meet the needs of the workplace. The Professional Skills developed by business and industry leaders across Arizona are integrated throughout the program. Network Security students develop leadership, social, civic, and career skills through participation in the state-recognized Career and Technical Student Organizations, SkillsUSA or FBLA (Future Business Leaders of America).

The Network Security instructional program prepares students for entry-level employment, further training, and/or post-secondary education for these and other occupations: Cryptologic Technician, Cyber Risk, Manager, Hardware Technician/Engineer, Help Desk Technician/Manager, Intelligence Analysis Intern, IT Designer, Network Technician, Administrator Technician, Analyst Technician, PC Technician, Program Analyst Systems Analyst, Systems Operations Specialist, Technical Sales Representative, Technical Support Technician/Manager, Training Manager, and Wireless Network Specialist.

INDUSTRY CREDENTIALS
The following credentials have been approved for the A-F CCR and are CTED eligible for the Network Security instructional program:

- CompTIA - A+
- CompTIA - IT Fundamentals
- CompTIA - Network+
- CompTIA - Security +
- CSX Cybersecurity Fundamentals Certificate

The following industry credentials have been approved to meet CTED eligibility for the Network Security instructional program:
- Certified Network Associate (CCNA) Routing and Switching Certification
- Client Pro (Windows 7-8 management troubleshooting certification)
- Global Security Essentials Certification (GSEC)
- Linux Pro (Linux prep certification)
- Microsoft Certified Professional (MCP)
- Network Pro (networking basics)
- Network +
- Security Pro (entry-level IT security administrator)
- Server Pro (Windows server skills)
- TestOut PC Pro Certification

**COHERENT SEQUENCE**
- 11.1999.12 – Network Security I, and
- 11.1999.30 – Network Security II, and program may elect to add:
  - 11.1999.35 – Network Security III, or
  - 11.1999.40 – Network Security IV, or
- 11.1999.71 – Network Security – DCE (Diversified Cooperative Education) or
- 11.1999.76 – Network Security – Internship, or

**TEACHER CERTIFICATION REQUIREMENTS**
The instructor must be ADE/CTE certified in one of the following Certificates:
- SCTBM Standard Career and Technical Education Business and Marketing
- SSCTEBM Standard Specialized Career and Technical Education Business and Marketing
- SCTIET Standard Career and Technical Education Industrial and Emerging Technologies
- SSCTEIET Standard Specialized Career and Technical Education Industrial and Emerging Technologies

Note:
- Network Security 11.1999.71 (DCE) requires a CTE Teacher to have the Cooperative Education Endorsement (CEN).
- Network Security 11.1999.76 (Internship) does not require a CTE Teacher to have a Cooperative Education Endorsement (CEN).
- Network Security 11.1999.81 (Cooperative Ed.) requires CTE Teachers to be appropriately certified for the program and to have a Cooperative Education Endorsement (CEN). (CTE Program Area Requirements, 2023).
Appendix O: Network Security 11.1999.00 Blueprint

**Blueprint for Instruction and Assessment**
**Network Security**
11.1999.00

<table>
<thead>
<tr>
<th>Domain</th>
<th>Related Standards</th>
<th>Instructional Time</th>
</tr>
</thead>
</table>
| Domain 1         | **STANDARD 1.0 APPLY PROBLEM-SOLVING AND CRITICAL THINKING SKILLS TO NETWORK SECURITY**  
| Network Essentials | **STANDARD 9.0 DEMONSTRATE BASIC COMPUTER MATHEMATICS REQUIRED FOR NETWORK SECURITY**  
|                  | **STANDARD 8.0 DESCRIBE NETWORK PROTOCOLS AND STANDARDS**                        | 45-55%            |
|                  | **STANDARD 9.0 CONFIGURE A BASIC NETWORK**                                        |                   |
|                  | **STANDARD 11.0 PERFORM NETWORK MAINTENANCE AND RESOLVE ISSUES**                  |                   |
| Domain 2         | **STANDARD 7.0 DEMONSTRATE NETWORK MEDIA AND TOPOLOGIES**                         | 25-35%            |
| Devices and Framework |                                                |                   |
| Domain 3         | **STANDARD 3.0 SPECIFY NETWORK SECURITY BEST PRACTICES, RISKS, AND THREATS**      | 15-25%            |
| Network Security | **STANDARD 4.0 INVESTIGATE LEGAL AND ETHICAL ISSUES RELATED TO NETWORK SECURITY** |                   |
|                  | **STANDARD 8.0 DESCRIBE THE DEVELOPMENT AND EVOLUTION OF COMPUTERS AND NETWORK SECURITY** |                   |
| Domain 4         | **STANDARD 2.0 MAINTAIN A SAFE AND ENVIRONMENTALLY CONSCIOUS WORK ENVIRONMENT**    | 5-15%             |
| Infrastructure Security |                                               |                   |

Content domains are bodies of knowledge, skills, or abilities to be taught and assessed. They illustrate the relationship among technical standards, instructional time, and student success on the Technical Skills Assessment. This blueprint corresponds with the technical standards endorsed on July 14, 2019.

(Blueprint, 2019).
## Appendix P: Network Security 11.1999.00 Instructional Framework

### Instructional Framework

**Network Security 11.1999.00**

This Instructional Framework identifies, explains, and expands the content of the standards/measurement criteria, and, as well, guides the development of multiple-choice items for the Technical Skills Assessment. This document corresponds with the Technical Standards endorsed on July 14, 2019.

#### Domain 1: Network Essentials

**Instructinal Time: 45-55%**

<table>
<thead>
<tr>
<th>STANDARD</th>
<th>APPLY PROBLEM-SOLVING AND CRITICAL THINKING SKILLS TO NETWORK SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Describe methods to determine priorities in establishing and maintaini</td>
</tr>
<tr>
<td></td>
<td>Design</td>
</tr>
<tr>
<td></td>
<td>Document</td>
</tr>
<tr>
<td></td>
<td>Testing (equipment verification, connectivity)</td>
</tr>
<tr>
<td></td>
<td>Baseline (testing variances and limits)</td>
</tr>
<tr>
<td>1.2</td>
<td>Prepare a plan of work and schedule network technology tasks</td>
</tr>
<tr>
<td></td>
<td>Prioritize</td>
</tr>
<tr>
<td></td>
<td>Trouble tickets</td>
</tr>
<tr>
<td></td>
<td>Daily routine tasks (check logs, equipment, and software updates, etc.)</td>
</tr>
<tr>
<td>1.3</td>
<td>Apply problem-solving processes to network technology tasks (i.e., bottom-up, divide-and-conquer, top-down, etc.)</td>
</tr>
<tr>
<td></td>
<td>Scenario based - use network problem to teach:</td>
</tr>
<tr>
<td></td>
<td>- Bottom-up</td>
</tr>
<tr>
<td></td>
<td>- Top-down</td>
</tr>
<tr>
<td></td>
<td>- Divide-and-conquer</td>
</tr>
<tr>
<td>1.4</td>
<td>Prepare and present technical information for non-technical and technical audiences in writing and verbally</td>
</tr>
<tr>
<td></td>
<td>Document and present at a technical and non-technical level</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STANDARD</th>
<th>DEMONSTRATE BASIC COMPUTER MATHEMATICS REQUIRED FOR NETWORK SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Explain the function of base number systems in mathematics as it relates to network technology</td>
</tr>
<tr>
<td></td>
<td>Base 10</td>
</tr>
<tr>
<td></td>
<td>Base 2</td>
</tr>
<tr>
<td></td>
<td>Base 16</td>
</tr>
<tr>
<td>5.2</td>
<td>Perform decimal to binary and binary to decimal conversions</td>
</tr>
<tr>
<td></td>
<td>Decimal to binary and binary to decimal conversions</td>
</tr>
<tr>
<td>5.3</td>
<td>Perform decimal to hexadecimal and hexadecimal to decimal conversions</td>
</tr>
<tr>
<td></td>
<td>Decimal to hexadecimal and hexadecimal to decimal conversions</td>
</tr>
<tr>
<td>5.4</td>
<td>Perform hexadecimal to binary and binary to hexadecimal conversions</td>
</tr>
<tr>
<td></td>
<td>Hexadecimal to binary and binary to hexadecimal conversions</td>
</tr>
<tr>
<td>5.5</td>
<td>Determine the appropriate method to perform conversions (e.g., paper-pencil and electronic resources)</td>
</tr>
<tr>
<td></td>
<td>Programming calculator</td>
</tr>
<tr>
<td></td>
<td>Subnet calculator</td>
</tr>
<tr>
<td>5.6</td>
<td>Apply basic Boolean logic for actions such as Google searches and scripting (e.g., –, &quot;and,&quot; &quot;nor,&quot; &quot;nor,&quot; and &quot;or&quot;)</td>
</tr>
<tr>
<td></td>
<td>Scripting (i.e., Write batch files, etc.)</td>
</tr>
<tr>
<td></td>
<td>Boolean logic: &quot;and,&quot; &quot;nor,&quot; &quot;nor,&quot; and &quot;or&quot;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STANDARD</th>
<th>DESCRIBE NETWORK PROTOCOLS AND STANDARDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1</td>
<td>Describe the parts and use of a Media Access Control (MAC) address</td>
</tr>
<tr>
<td></td>
<td>- MAC address length</td>
</tr>
<tr>
<td></td>
<td>- QUIT</td>
</tr>
<tr>
<td></td>
<td>- IEEE 802</td>
</tr>
<tr>
<td>8.2</td>
<td>Describe the characteristics, name, and use of the seven layers of the Open Systems Interconnect (OSI) model</td>
</tr>
<tr>
<td></td>
<td>- Open Systems Interconnect (OSI) model</td>
</tr>
<tr>
<td>8.3</td>
<td>Describe the characteristics, name, and use of the four layers of the Transmission Control Protocol/Internet Protocol (TCP/IP) model</td>
</tr>
<tr>
<td></td>
<td>- Characteristics and names of the four layers of the Transmission Control Protocol/Internet Protocol (TCP/IP) model</td>
</tr>
<tr>
<td>8.4</td>
<td>Explain the purpose of dynamic and static routing protocols</td>
</tr>
<tr>
<td></td>
<td>- Purpose of dynamic and static routing protocols</td>
</tr>
<tr>
<td>8.5</td>
<td>Explain the concept of ports and identify the three port ranges used in networking services and protocols (i.e., dynamic/private [49152-65535], system [0-1023], user [1024-49151], etc.)</td>
</tr>
<tr>
<td></td>
<td>- Concepts of ports and identify the three port ranges used in networking services and protocols:</td>
</tr>
<tr>
<td></td>
<td>- Dynamic/private [49152-65535]</td>
</tr>
<tr>
<td></td>
<td>- System [0-1023]</td>
</tr>
<tr>
<td></td>
<td>- User [1024-49151]</td>
</tr>
<tr>
<td>8.6</td>
<td>Describe standard network ports and protocols (e.g., Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), File Transfer Protocol (FTP), HyperText Transfer Protocol (HTTP), Point-of-Presence (POP), Simple Mail Transfer Protocol (SMTP), etc.)</td>
</tr>
<tr>
<td></td>
<td>- Acronyms:</td>
</tr>
<tr>
<td></td>
<td>- Domain Name System (DNS)</td>
</tr>
<tr>
<td></td>
<td>- Dynamic Host Configuration Protocol (DHCP)</td>
</tr>
<tr>
<td></td>
<td>- File Transfer Protocol (FTP)</td>
</tr>
<tr>
<td></td>
<td>- HyperText Transfer Protocol (HTTP)</td>
</tr>
<tr>
<td></td>
<td>- Point-of-Presence (POP)</td>
</tr>
<tr>
<td></td>
<td>- Simple Mail Transfer Protocol (SMTP), etc.</td>
</tr>
<tr>
<td>8.7</td>
<td>Describe the applications and characteristics of Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)</td>
</tr>
<tr>
<td></td>
<td>- Stateful</td>
</tr>
<tr>
<td></td>
<td>- Stateless</td>
</tr>
</tbody>
</table>
8.6 Differentiate IPv4/IPv6 addresses and their corresponding subnet masks (i.e., classful networks, Classless Interdomain Routing (CIDR), private vs public IP)

- Classful networks
- Classless Interdomain Routing (CIDR)
- Private IP
- Public IP

8.9 Summarize the basic characteristics and protocols of Metropolitan Area Network (MAN), Software Defined Wide Area Network (SD-WAN), and Wide Area Network (WAN) technologies (i.e., Asynchronous Transfer Mode (ATM), frame relay, Multiprotocol Label Switching (MPLS), etc.)

- Basic characteristics and protocols
  - Metropolitan Area Network (MAN)
  - Software Defined Wide Area Network (SD-WAN)
  - Wide Area Network (WAN) technologies
  - Asynchronous Transfer Mode (ATM)
  - Frame relay
  - Multiprotocol Label Switching (MPLS)

8.10 Describe remote access protocols and services

- Remote access protocols and services

8.11 Describe the function and purpose of security protocols (i.e., Hypertext Transfer Protocol Secure (HTTPS), Secure File Transfer Protocol (SFTP), tunnelling, Virtual Private Network (VPN), etc.)

- Function and purpose of security protocol
  - Hypertext Transfer Protocol Secure (HTTPS)
  - Secure File Transfer Protocol (SFTP)
  - Tunnelling
  - Virtual Private Network (VPN), etc.

8.12 Explain the importance of proper documentation in accordance with industry standards

- Physical topology
- Logical topology
- End-user agreement documentation

STANDARD 3.0 CONFIGURE A BASIC NETWORK

9.1 Design a network map with virtual and physical segments

- VLAN

9.2 Construct dynamic and static routes

- Dynamic and static routes

9.3 Explain proper labelling in accordance with industry standards (i.e., cable, device, rack, wall plates, etc.)

- Proper labelling in accordance with industry standards
  - Cable
  - Device
  - Rack
  - Wall plates, etc.

9.4 Describe the components needed and purpose to build fault tolerance into a network

- Fault tolerance and redundancy
  - Mesh
  - Failover
  - Port forwarding

9.5 Describe the purpose of a disaster recovery plan for a network

- Offsite storage
- Documentation

9.6 Install and configure a physical and/or virtual networked system (i.e., Linux/UNIX, Windows, etc.)

- VMware
- VirtualBox (free software)

9.7 Configure network cards, network settings, and operating system

- Configure
  - Network cards
  - Network settings
  - Operating system

9.8 Configure and connect devices to the network (i.e., computers, printers, routers, switches, etc.)

- Configure and connect devices to the network
  - Computers
  - Printers
  - Routers
  - Switches

9.9 Identify the appropriate tools to use for diagnostic tasks or network repair (i.e., execute Traceroute, Ipconfig, Ping, etc.)

- Appropriate tools to use for diagnostic tasks or network repair
  - Traceroute
  - Ipconfig
  - Ping

STANDARD 11.0 PERFORM NETWORK MAINTENANCE AND RESOLVE ISSUES

11.1 Identify maintenance tasks and create a schedule

- Prioritize
- Trouble tickets
- Daily routine tasks (check logs, equipment, and software updates, etc.)

11.2 Describe the purpose and benefits of network utilities (i.e., Network Statistics (Netstat), Name Server Lookup (Nslookup), Ping, Traceroute, etc.)

- Network utilities
  - Network Statistics (Netstat)
  - Name Server Lookup (Nslookup)
  - Ping
  - Traceroute, etc.

11.3 Demonstrate the use of visual indicators (i.e., indicator lights on devices, etc.) and diagnostic utilities (i.e., Wireshark, etc.) to interpret problems

- Network utilities
  - Network Statistics (Netstat)
  - Name Server Lookup (Nslookup)
  - Ping
  - Traceroute, etc.
### Domain 2: Devices and Framework

**Instructional Time: 25-35%**

**STANDARD 7.8 DEMONSTRATE NETWORK MEDIA AND TOPOLOGIES**

| 7.1 Specify the characteristics and main features of various networking topologies (e.g., bus, mesh, ring, and star) | - Bus  
- Mesh  
- Ring  
- Star |
|---|---|
| 7.2 Compare and contrast proper physical network topology | - Physical network topology  
- Bus  
- Ring  
- Star  
- Hybrid |
| 7.3 Identify appropriate connectors, media types, and uses for various networks | - RJ45 Female  
- RJ45 Male BRIC (8 Position, 8 Contact) |

| 7.4 Compare and contrast physical and virtual networks (i.e., Software-Defined Wide-Area Network (SD-WAN), Virtual Local Area Network (VLAN), etc.) | - Software-Defined Wide-Area Network (SD-WAN)  
- Virtual Local Area Network (VLAN) |
|---|---|
| 7.5 Specify the characteristics of physical network technologies including cable types, length, speed, and topology | - CAT3  
- CAT5  
- CAT6  
- CAT6A  
- CAT4  
- 10BASE5 (100)  
- 100BASE5 (10)  
- FIBER |
| 7.6 Specify the characteristics of wireless network technologies including frequency, speed, topology, and transmission (i.e., local area, metropolitan area, wide area networks, etc.) | - 02.11 |
| 7.7 Describe the structure of the internet (network of networks) | - Hierarchy  
- LAN to WAN |
| 7.8 Identify the features, functions, and purpose of commonly used network components (i.e., routers, modem, switches, bridges, hubs, NIC (network interface card), etc.) | - Bottom-up  
- NIC  
- Computer  
- Switch  
- Router |

### Domain 3: Network Security

**Instructional Time: 15-25%**

**STANDARD 8.9 SPECIFY NETWORK SECURITY BEST PRACTICES, RISKS, AND THREATS**

| 3.1 Perform risk management activities (e.g., define risk, determine risk level, and identify methods to address risk) | - Define risk  
- Determine risk level  
- Identify methods to address risk (mitigation) |
|---|---|
| 3.2 Define policies to manage system and data availability, confidentiality, and integrity | - End-user agreements  
- Physical security  
- ACLs  
- Group policies |
| 3.3 Classify data according to its sensitivity and criticality (i.e., mission critical, protect cafeteria menu vs. personal, financial and health information, trade secrets, etc.) | • File sharing  
• Other topics as needed  
• Prioritize the severity of data lost |
| 3.4 Identify security threats related to computer data, hardware, and software (i.e., denial of service, eavesdropping, intrusion, unauthorized access, unauthorized use, etc.) | • Security threats  
  o Denial of service  
  o Eavesdropping  
  o Intrusion  
  o Unauthorized access  
  o Unauthorized use |
| 3.5 Explain the importance of physical security of computer and network hardware following best practices (i.e., cameras, locks, USB port blocking, etc.) | • Physical security |
| 3.6 Describe network threats (i.e., denial of service, email spoofing, hacking/tracking, intrusion, malware, phishing, social engineering, spamming, system vulnerabilities, website defacement, etc.) | • Social engineering |
| 3.7 Describe best practices to protect against network threats (i.e., access control, antivirus software, awareness and training, encryption, firewalls, incident detection systems/tools, intrusion detection prevention, network segmentation, port/service blocking, software updates/patches, etc.) | • Access control  
• Antivirus software  
• Awareness and training  
• Encryption  
• Firewalls  
• Incident detection systems/tools  
• Intrusion detection prevention  
• Network segmentation  
• Port/service blocking  
• Software updates/patches, etc. |
| 3.8 Define best practices to protect data at rest, data in transit, and data during processing | • Encryption  
• Tunneling |
| 3.9 Describe password best practices (i.e., age, complexity, history, length, lockout, etc.) | • Password best practices  
  o Age  
  o Complexity  
  o History  
  o Length  
  o Lockout |
| 3.10 Analyze authentication methods used to secure access to the network (i.e., biometrics, key cards, multi-factor authentication (MFA), passwords, single sign-on (SSO), two-factor authentication (2FA), etc.) | • Authentication methods to secure access to the network  
  o Biometrics  
  o Key cards  
  o Multi-factor authentication (MFA)  
  o Passwords, single sign-on (SSO)  
  o Two-factor authentication (2FA) |
| 3.11 Identify best practices for access control (i.e., changing default passwords, disabling unused accounts, least privileges, privileged account management, role-based access control, etc.) | • Access control best practices  
  o Changing default passwords  
  o Disabling unused accounts  
  o Least privileges  
  o Privileged account management  
  o Role-based access control |

**STANDARD 4.0 INVESTIGATE LEGAL AND ETHICAL ISSUES RELATED TO NETWORK SECURITY**

| 4.1 Explore issues regarding intellectual property rights including software licensing and software duplication (i.e., Business Software Alliance, Creative Commons, Digital Right Management (DRM)), https://www.ip-watch.org/about/, https://www.refl.org/, etc. | • Copyright laws |
| 4.2 Differentiate among freeware, open source, proprietary, and shareware software relative to legal and ethical issues | • Open source  
• Closed source |
| 4.3 Identify issues, laws, and trends affecting data and privacy (e.g., General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), and Sarbanes-Oxley Act (SOX)) | • Torrrenting  
• HIPAA |
| 4.4 Describe acceptable use of industry-related data, private and public networks, and social networking | • Acceptable use of:  
  o Industry-related data  
  o Private networks  
  o Public networks  
  o Social networking |

**STANDARD 6.0 DESCRIBE THE DEVELOPMENT AND EVOLUTION OF COMPUTERS AND NETWORK SECURITY**

| 6.1 Describe a computer and its components and function | • Computer components and functions |
| 6.2 Explain the historical evolution of the computer and computer networks | • ARPAnet  
• Computer and network timeline |
6.3 Explain how the development of computers has impacted modern life

- Development of computers has impacted modern life
  - FOMO (Fear of Missing Out)
  - Cell phone withdrawal, etc.

6.4 Identify the components and structure of an information system (e.g., applications, media (cables, fiber, and wireless), network devices (router, switches, etc.), operating systems, and servers)

- Components and structure of an information system
  - Applications
  - Media (cables, fiber, and wireless)
  - Network devices (router, switches, etc.)
  - Operating systems and servers

6.5 Discuss future trends and societal impacts in digital devices and network technology (i.e., Internet of Things (IoT), privacy, etc.)

- Internet of Things (IoT)

**Domain 4: Infrastructure Security**

**Instructional Time: 5-15%**

**STANDARD 2.9 MAINTAIN A SAFE AND ENVIRONMENTALLY CONSCIOUS WORK ENVIRONMENT**

2.1 Identify personal responsibility for developing and maintaining a safe and healthy work environment

- OSHA
- AZ Professional Skills

2.2 Use equipment, materials, and tools commonly used in the field of network security correctly and safely

- Crimper
- Cable tester
- Punch down tool
- PPE (Personal Protection Equipment)
- ESD strip
- Wire cutters

2.3 Identify ergonomic solutions to prevent injuries common to network security tasks

- Ergonomic solutions to prevent injuries
  - Carpal tunnel
  - Repetitive action, etc.

2.4 Determine safe working practices to avoid or eliminate electrical hazards and physical injuries

- Grounding and bonding

2.5 Identify techniques used to manage power consumption in the networked environment (i.e., cloud-based, software defined, etc.)

- Cloud-based
- Software defined
- Power management settings

2.6 Explain environmental considerations when disposing of computer/network components

- EPA (Environmental Protection Agency)

2.7 Describe and resolve most common electrostatic discharge (ESD) hazards in a network environment

- Generators
- Fluorescent light ballasts
- Microwaves, etc.

**STANDARD 10.0 HARDEN A NETWORK**

10.1 Identify common network threats (i.e., denial of service, eavesdropping, intrusion, probing, unauthorized access, etc.)

- Denial of service
- Eavesdropping
- Intrusion
- Probing
- Unauthorized access

10.2 Identify physical network threats (i.e., disrupting media (like cutting fiber), environmental/power disruption, unauthorized access to devices, etc.)

- Disrupting media (similar to cutting fiber)
- Environmental/power disruption
- Unauthorized access to devices, etc.

10.3 Describe the benefits and purpose of segmenting networks

- VLAN
- IP subnetting (VLSM)

10.4 Describe the benefits of disabling ports and network services

- Authorized access
- MAC address filtering
- HTTP vs. HTTPS
- FTP vs. SFTP

10.5 Describe the techniques to secure a Wi-Fi network (i.e., Extensible Authentication Protocol (EAP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2), etc.)

- SSID
- Default password
- Default IP address
- WPA
- WEP
- WEP2

10.6 Compare and contrast the various types of firewalls and their uses (i.e., application, packet filtering, stateful, etc.)

- Application, packet filtering, stateful
- Hardware and software firewalls

10.7 Describe the benefits, disadvantages, and purpose of using a proxy service

- Benefits, disadvantages
- Purpose of using a proxy service
<table>
<thead>
<tr>
<th>10.5 Describe the benefits, disadvantages, and purpose of using network intrusion detection/prevention systems [i.e., Intrusion Detection System / Intrusion Prevention System (IDS/IPS), etc.]</th>
<th>• Intrusion Detection System / Intrusion Prevention System (IDS/IPS), etc.</th>
</tr>
</thead>
</table>
| 10.9 Modify an existing network diagram with appropriate network hardening devices or systems | • “Harden” network:  
  - Proxy server  
  - VPN  
  - Firewall  
  - ACLs  
  - Intrusion Protection |