Unit 1: Foundations and Threats

Content Area: **Applied Tech**
Course(s): **Generic Course**
Time Period: **Marking Period 1**
Length: **4 weeks**
Status: **Published**

Standards

Life Literacies and Key Skills

TECH.9.4.12.CI.2	Identify career pathways that highlight personal talents, skills, and abilities (e.g., 1.4.12prof.CR2b, 2.2.12.LF.8).
TECH.9.4.12.CI.3	Investigate new challenges and opportunities for personal growth, advancement, and transition (e.g., 2.1.12.PGD.1).
TECH.9.4.12.DC.3	Evaluate the social and economic implications of privacy in the context of safety, law, or ethics (e.g., 6.3.12.HistoryCA.1).
TECH.9.4.12.DC.4	Explain the privacy concerns related to the collection of data (e.g., cookies) and generation of data through automated processes that may not be evident to users (e.g., 8.1.12.NI.3).
TECH.9.4.12.DC.5	Debate laws and regulations that impact the development and use of software.
TECH.9.4.12.TL.1	Assess digital tools based on features such as accessibility options, capacities, and utility for accomplishing a specified task (e.g., W.11-12.6.).

Computer Science Standards

CS.9-12.8.1.12.CS.1	Describe ways in which integrated systems hide underlying implementation details to simplify user experiences.
CS.9-12.8.1.12.CS.2	Model interactions between application software, system software, and hardware.
CS.9-12.8.1.12.IC.1	Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.
CS.9-12.8.1.12.IC.3	Predict the potential impacts and implications of emerging technologies on larger social, economic, and political structures, using evidence from credible sources.
CS.9-12.8.1.12.NI.2	Evaluate security measures to address various common security threats.
CS.9-12.8.1.12.NI.3	Explain how the needs of users and the sensitivity of data determine the level of security implemented.
CS.9-12.8.1.12.NI.4	Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.

Transfer Goals and Career Ready Practices

Transfer Goals

Students will be able to independently use their learning to identify security threats and determine the best practices for protecting against malicious software.

Concepts

Essential Questions

- What is the CIA Triad?
- How is malware used to impact systems and people?
- What is the goal of cybersecurity?
- Why do most cybersecurity professionals use a command line interface?

Understandings

Students will understand that...

- Authentication is a key tool in protecting data.
- Ethics are an important element of cybersecurity.
- The goal of cybersecurity is to protect CIA of data at rest, in transit and in use.
- There are many reasons for pursuing cybersecurity career and motivations, such as job demand, protect society, income, etc.

Critical Knowledge and Skills

Knowledge

Students will know:

• Cybersecurity

• CIA Triad

• Confidentiality

• Integrity

- Availability
- Authentication
- Access Control
- Accounting
- Password
- Single Sign-On (SSO)
- Breach
- Database
- Dictionary Attack
- Brute force attack
- Hybrid Attack
- Password Spraying
- Credentials
- Credential Stuffing
- Identify Proofing
- Passphrases
- Hashing
- Rainbow Tables
- Hash collision
- Birthday Attack
- Smart Cards
- Certificate
- Algorithm
- Biometrics
- Malware
- Virus
- Worm
- Replicates
- Trojan
- RAT – Remote Access Trojan
- Backdoor

• BOTNET
• Logic Bomb
• Rootkit
• Zero Day
• Vulnerability Window
• APT – Advanced Persistent Threat
• Exfiltrate
• Ransomware
• Spyware
• Adware
• PUP / PUA
• SPAM
• Virtualization
• Hypervisor
• Host
• Host OS
• Virtual Machine
• Virtualization software
• Command Line
• Graphical User Interfaces
• Linux
• Specialized operating system
• Terminal
• Prompt
• Path

Skills

Students will be able to:

• Explore reasons for pursuing a cybersecurity career
• Understand content of coursework
• Understand the class Ethics agreement

• Identify the key goals and frameworks of Cybersecurity
• Identify the CIA Triad as the characteristics of information
• Identify the state of information as stored, transmission, and processing

• Identify the types of malicious software that exist and how they can be layered to increase the security threat
• Examine how malware has a negative impact on a computer system and on a person

• Identify the characteristics of virtualization software
• Apply steps to open and configure Virtual Machines
• Confirm access to online VMs

Assessment and Resources

Primary Resources

Intro to Cybersecurity

hosted by cyber.org

available online at https://cyber.instructure.com/courses/243

Supplementary Resources

- cyber.org Cyber Range
- NJ Brookdale CC Cyber Range
- CyberStart America

School Summative Assessment Plan

- Unit Assessment
- Unit Labs
- Unit Project

School Formative Assessment Plan (Other Evidence)

- Guided Notes
- Lesson Activities
- Worksheets

Technology Integration and Differentiated Instruction

Technology Integration

- **Google Products**
    - Google Classroom - Used for daily interactions with the students covering a vast majority of different educational resources (Daily Notes, Exit Tickets, Classroom Polls, Quick Checks, Additional Resources/ Support, Homework, etc.)
    - GAFE (Google Apps For Education) - Using various programs connected with Google to collaborate within the district, co-teachers, grade level partner teacher, and with students to stay connected with the content that is covered within the topic. Used to collect data in real time and see results upon completion of the assignments to allow for 21st century learning.

- **One to One Student's laptop**
    - All students within the West Deptford School District are given a computer, allowing for 21st century learning to occur within every lesson/topic.

- **Virtual Machines**
    - Students will use virtual machines to demonstrate, test, and analyze different cyber attacks.

Differentiated Instruction

Gifted Students (N.J.A.C.6A:8-3.1)

❑ Within each lesson, the Gifted Students are given choice on topic and subject matter allowing them to explore interests appropriate to their abilities, areas of interest and other courses.

English Language Learners (N.J.A.C.6A:15)

❑ Within each lesson, the English Language Learners are given choice of topic and resources so that their materials are within their ability to grasp the language.

❑ All assignments have been created in the student's native language.

❑ Work with ELL Teacher to allow for all assignments to be completed with extra time.

At-Risk Students (N.J.A.C.6A:8-4.3c)

❑ Within each lesson, the at-risk students are given choice of topic and resources so that their materials

are within their ability level and high-interest.

Special Education Students (N.J.A.C.6A:8-3.1)

❑ Within each lesson, special education students are given choice of topic and resources so that their materials are within their ability level and high-interest.

❑ All content will be modeled with examples and all essays are built on a step-by-step basis so modifications for assignments in small chunks are met.

All other IEP modifications will be honored (ie. hard copies of notes, directions restated, etc.)

Interdisciplinary Connections

- Computer Science: Cybersecurity is closely related to computer science as it involves the study of algorithms, data structures, programming languages, and network protocols. Understanding the technical aspects of cybersecurity requires knowledge of computer systems, software development, and encryption techniques.

- Mathematics: Mathematics plays a crucial role in cybersecurity. Concepts such as cryptography, probability theory, and discrete mathematics are fundamental to designing secure algorithms and encryption methods. Understanding mathematical concepts helps in analyzing the strength and vulnerabilities of cryptographic systems.

- Psychology: Cybersecurity involves understanding the motivations and behaviors of hackers, as well as the psychology of individuals targeted by cyberattacks. Psychological concepts such as social engineering, human factors in security, and user behavior play a vital role in designing secure systems and raising awareness about cyber threats.

- Law and Ethics: Cybersecurity is closely tied to legal and ethical considerations. Understanding laws and regulations related to data protection, privacy, intellectual property, and cybercrime is crucial for cybersecurity professionals. Ethical considerations, such as responsible disclosure and the ethics of hacking, are also important topics to explore.

- Business and Management: Cybersecurity has become a critical concern for businesses of all sizes. Understanding cybersecurity risks and developing effective strategies to protect organizational assets requires knowledge of business management principles, risk assessment, and incident response planning. It also involves considering the economic impact of cyber threats on businesses.

- Sociology: Cybersecurity is not solely a technical issue but also a sociological one. Analyzing the societal impact of cyber threats, studying cybercrime patterns, and understanding the social dynamics of online communities are essential for addressing cybersecurity challenges effectively. Sociological perspectives also shed light on issues related to privacy, surveillance, and trust in the digital world.

- Communication Studies: Effective communication is crucial in cybersecurity. Being able to

communicate complex technical concepts, risks, and mitigation strategies to both technical and non-technical stakeholders is essential. Studying communication theories, rhetoric, and persuasive techniques helps cybersecurity professionals convey their message clearly and influence behavior change.

- Economics: Cybersecurity has economic implications for individuals, organizations, and society as a whole. Analyzing the cost of cyberattacks, evaluating the return on investment for cybersecurity measures, and understanding the economic incentives behind cybercrime provide valuable insights for designing effective cybersecurity strategies.

- Political Science: Cybersecurity intersects with political science as it involves national security, cyber warfare, and international cooperation on cybersecurity issues. Studying international relations, government policies, and the role of state actors in cyber conflicts helps in understanding the broader context of cybersecurity challenges.

- Education: Cybersecurity education and awareness are crucial for building a cyber-resilient society. Incorporating educational theories, instructional design, and pedagogical strategies into cybersecurity training programs helps in effectively teaching individuals to protect themselves and their organizations from cyber threats.

Learning Plan / Pacing Guide

Course Notes:
• 1 day is ~ a 42-45 minute lesson that meets 5 days per week
• Lessons have several types of learning outside of lecture. These abbreviations are used as a reference: (G) Group activity) (L) Lab online (A) Activity
0.1 First Day Info & Ethics Agreement – 1 day
1. Careers – introduction to reasons for pursuing cybersecurity career and motivations such as job demand, protect society, income, etc.
2. Review what will be covered in class – objectives handout to determine what students find most and least interesting
3. Ethics agreement – (G) group work to create a Code of Behavior. Present and discuss why we need one. Review real Ethics Agreement for understanding of expectations and consequences.

1.1 CIA Triad and Authentication – 7 days
1. Cybersecurity goal is to protect CIA of data at rest, in transit and in use.
2. Define Authentication as a key tool - explore methods including strong passwords, tokens, MFA and biometrics
3. Identify attacks on passwords and use of salted hashes as defense.
Activities: (L) Testing passwords, (L) Have You Been Pwned (L) CyberChef tool to hash & salt with CyberChef Intro Video (A) Create safe password poster, (G) Which Authentication project.

1.2 Identifying Security Threats – 6 days
1. Define types of malware and the complexity of threats
2. Examine impact on systems and on people.
3. Summarize the best practices for protecting against malicious software
Activities: (A/G) Historic Malware Research/Presentation , (L) Rapper or Malware online game

1.3 Intro to Command Line – 6 days

1. Define difference between GUI and CLI
2. Learn basic terminal commands in Linux
3. Introduce Virtualization and how to use the course VMs

Activities: (L) Terminus game part 1, (L) Try It follow along with PPT

Unit 2: Human Factor

Content Area: **Applied Tech**
Course(s): **Generic Course**
Time Period: **Marking Period 1**
Length: **2 weeks**
Status: **Published**

Standards

Life Literacies and Key Skills

TECH.9.4.12.DC.4	Explain the privacy concerns related to the collection of data (e.g., cookies) and generation of data through automated processes that may not be evident to users (e.g., 8.1.12.NI.3).
TECH.9.4.12.DC.6	Select information to post online that positively impacts personal image and future college and career opportunities.
TECH.9.4.12.TL.1	Assess digital tools based on features such as accessibility options, capacities, and utility for accomplishing a specified task (e.g., W.11-12.6.).

Computer Science Standards

CS.9-12.8.1.12.IC.1	Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.
CS.9-12.8.1.12.NI.2	Evaluate security measures to address various common security threats.
CS.9-12.8.1.12.NI.3	Explain how the needs of users and the sensitivity of data determine the level of security implemented.

Transfer Goals and Career Ready Practices

Transfer Goals

Students will be able to independently use their learning to mitigate human risk in cybersecurity.

Concepts

Essential Questions

- What role does social engineering play in cybersecurity?
- How can human risk be mitigated?

Understandings

Students will understand that...

- The most vulnerable part of most systems are the users.
- Human risk can be mitigated through the use of awareness, well-written policies, and training.
- Phishing is the most common method of hacking.

Critical Knowledge and Skills

Knowledge

Students will know:

• Social Engineering
• Hacking
• Baiting
• Shoulder surfing
• Piggybacking
• Dumpster diving
• Vishing
• Pretexting
• Scareware

• Phishing
• Spear-phishing
• Whaling
• Smishing
• Vishing
• OSINT
• Reverse Social Engineering
• Hoaxes
• Mitigate
• Policy
• Procedure

Skills

Students will be able to:

• Identify some common steps used in typical digital attacks
• Define social engineering as the human risk in organization security
• Identify techniques for social engineering and how to mitigate against these techniques

• Define phishing as a primary tool in social engineering
• Identify special types and characteristics of phishing

Assessment and Resources

Primary Resources

Intro to Cybersecurity

hosted by cyber.org

available online at https://cyber.instructure.com/courses/243

Supplementary Resources

- cyber.org Cyber Range
- NJ Brookdale CC Cyber Range
- CyberStart America

School Summative Assessment Pan

- Unit Assessment
- Unit Labs
- Unit Project

School Formative Assessment Plan (Other Evidence)

- Guided Notes

- Lesson Activities
- Worksheets

Technology Integration and Differentiated Instruction

Technology Integration

● **Google Products**

- Google Classroom - Used for daily interactions with the students covering a vast majority of different educational resources (Daily Notes, Exit Tickets, Classroom Polls, Quick Checks, Additional Resources/ Support, Homework, etc.)
- GAFE (Google Apps For Education) - Using various programs connected with Google to collaborate within the district, co-teachers, grade level partner teacher, and with students to stay connected with the content that is covered within the topic. Used to collect data in real time and see results upon completion of the assignments to allow for 21st century learning.

● **One to One Student's laptop**

- All students within the West Deptford School District are given a computer, allowing for 21st century learning to occur within every lesson/topic.

● **Virtual Machines**

- Students will use virtual machines to demonstrate, test, and analyze different cyber attacks.

Differentiated Instruction

Gifted Students (N.J.A.C.6A:8-3.1)

❑ Within each lesson, the Gifted Students are given choice on topic and subject matter allowing them to explore interests appropriate to their abilities, areas of interest and other courses.

English Language Learners (N.J.A.C.6A:15)

❑ Within each lesson, the English Language Learners are given choice of topic and resources so that their materials are within their ability to grasp the language.

❑ All assignments have been created in the student's native language.

❑ Work with ELL Teacher to allow for all assignments to be completed with extra time.

At-Risk Students (N.J.A.C.6A:8-4.3c)

❑ Within each lesson, the at-risk students are given choice of topic and resources so that their materials are within their ability level and high-interest.

Special Education Students (N.J.A.C.6A:8-3.1)

❑ Within each lesson, special education students are given choice of topic and resources so that their materials are within their ability level and high-interest.

❑ All content will be modeled with examples and all essays are built on a step-by-step basis so modifications for assignments in small chunks are met.

All other IEP modifications will be honored (ie. hard copies of notes, directions restated, etc.)

Interdisciplinary Connections

- Computer Science: Cybersecurity is closely related to computer science as it involves the study of algorithms, data structures, programming languages, and network protocols. Understanding the technical aspects of cybersecurity requires knowledge of computer systems, software development, and encryption techniques.

- Mathematics: Mathematics plays a crucial role in cybersecurity. Concepts such as cryptography, probability theory, and discrete mathematics are fundamental to designing secure algorithms and encryption methods. Understanding mathematical concepts helps in analyzing the strength and vulnerabilities of cryptographic systems.

- Psychology: Cybersecurity involves understanding the motivations and behaviors of hackers, as well as the psychology of individuals targeted by cyberattacks. Psychological concepts such as social engineering, human factors in security, and user behavior play a vital role in designing secure systems and raising awareness about cyber threats.

- Law and Ethics: Cybersecurity is closely tied to legal and ethical considerations. Understanding laws and regulations related to data protection, privacy, intellectual property, and cybercrime is crucial for cybersecurity professionals. Ethical considerations, such as responsible disclosure and the ethics of hacking, are also important topics to explore.

- Business and Management: Cybersecurity has become a critical concern for businesses of all sizes. Understanding cybersecurity risks and developing effective strategies to protect organizational assets

requires knowledge of business management principles, risk assessment, and incident response planning. It also involves considering the economic impact of cyber threats on businesses.

- Sociology: Cybersecurity is not solely a technical issue but also a sociological one. Analyzing the societal impact of cyber threats, studying cybercrime patterns, and understanding the social dynamics of online communities are essential for addressing cybersecurity challenges effectively. Sociological perspectives also shed light on issues related to privacy, surveillance, and trust in the digital world.

- Communication Studies: Effective communication is crucial in cybersecurity. Being able to communicate complex technical concepts, risks, and mitigation strategies to both technical and non-technical stakeholders is essential. Studying communication theories, rhetoric, and persuasive techniques helps cybersecurity professionals convey their message clearly and influence behavior change.

- Economics: Cybersecurity has economic implications for individuals, organizations, and society as a whole. Analyzing the cost of cyberattacks, evaluating the return on investment for cybersecurity measures, and understanding the economic incentives behind cybercrime provide valuable insights for designing effective cybersecurity strategies.

- Political Science: Cybersecurity intersects with political science as it involves national security, cyber warfare, and international cooperation on cybersecurity issues. Studying international relations, government policies, and the role of state actors in cyber conflicts helps in understanding the broader context of cybersecurity challenges.

- Education: Cybersecurity education and awareness are crucial for building a cyber-resilient society. Incorporating educational theories, instructional design, and pedagogical strategies into cybersecurity training programs helps in effectively teaching individuals to protect themselves and their organizations from cyber threats.

Learning Plan / Pacing Guide

Course Notes:
• 1 day is ~ a 42-45 minute lesson that meets 5 days per week
• Lessons have several types of learning outside of lecture. These abbreviations are used as a reference:
(G) Group activity) (L) Lab online (A) Activity

2.1 Social Engineering – 2 days
1. Define steps hackers take in an attack
2. Define and explore social engineering as the human risk
Activities: (G or L) 7 Steps of an Attack – sorting, (L) CS Interactive: Social Engineering (L) Social Engineering Toolkit

---

2.2 Phishing & OSINT – 6 days
1. Define phishing, characteristics and specialized types.
2. Define Open Source Intelligence (OSINT) and explore the tools used in OSINT.
3. How to mitigate human risk – policies, awareness training, etc.
Activities: (L) Phishing test, (A) OSINT on Tony Stark, (L/A) Phishing Myself project, (L/G) Clean Desk Policy Mistakes

Unit 3: Data Safety and Best Practices

Content Area: **Applied Tech**
Course(s): **Generic Course**
Time Period: **Marking Period 1**
Length: **2 weeks**
Status: **Published**

Standards

Life Literacies and Key Skills

TECH.9.4.12.CI.3	Investigate new challenges and opportunities for personal growth, advancement, and transition (e.g., 2.1.12.PGD.1).
TECH.9.4.12.DC.4	Explain the privacy concerns related to the collection of data (e.g., cookies) and generation of data through automated processes that may not be evident to users (e.g., 8.1.12.NI.3).
TECH.9.4.12.DC.5	Debate laws and regulations that impact the development and use of software.
TECH.9.4.12.TL.1	Assess digital tools based on features such as accessibility options, capacities, and utility for accomplishing a specified task (e.g., W.11-12.6.).

Computer Science Standards

CS.9-12.8.1.12.CS.1	Describe ways in which integrated systems hide underlying implementation details to simplify user experiences.
CS.9-12.8.1.12.NI.2	Evaluate security measures to address various common security threats.
CS.9-12.8.1.12.NI.3	Explain how the needs of users and the sensitivity of data determine the level of security implemented.
CS.9-12.8.1.12.NI.4	Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.

Transfer Goals and Career Ready Practices

Transfer Goals

Students will be able to independently use their learning to reccommend best practices and examine vulnerabilities.

Concepts

Essential Questions

- What are the Best Practices configurations for typical PCs?
- How much risk is acceptable?
- What are some of the most common vulnerabilities?

Understandings

Students will understand that...

- Vulnerabilities and exploits are inherently intertwined.
- The Common Vulnerability and Exposure Database can be used as a research tool.
- Balancing risk against effort is an important part of cybersecurity.

Critical Knowledge and Skills

Knowledge

Students will know:

• Policy
• Devices
• Attack Vectors
• Mitigate
• Procedure
• Benchmarks
• Vulnerability assessment
• Patch / Update
• Hotfix
• Critical Update
• Security Update
• Scan
• Firewall
• User Access Control
• Services
• Least Privilege Principle
• Backup
• Redundancy
• System image
• Ransomware protection

• Threat Modeling
• Internet of Things (IoT)
• Smart device
• Embed
• Shodan IoT search engine

Skills

Students will be able to:

• Define and identify commonly seen types of vulnerabilities
• Examine how the Common Vulnerability and Exposure database can be used as a research tool

• Understand Threat Modeling to determine what risk you are willing to take and what effort you are willing to put in to secure your IOT devices.
• Examine vulnerabilities of home Internet of Things (IOT) – examples: robot vacuum, video doorbell, smart refrigerator, voice-activated virtual assistant, etc.

Assessment and Resources

Primary Resources

Intro to Cybersecurity

hosted by cyber.org

available online at https://cyber.instructure.com/courses/243

Supplementary Resources

- cyber.org Cyber Range
- NJ Brookdale CC Cyber Range
- CyberStart America

School Summative Assessment Plan

- Unit Assessment
- Unit Labs
- Unit Project

School Formative Assessment Plan (Other Evidence)

- Guided Notes
- Lesson Activities
- Worksheets

Technology Integration and Differentiated Instruction

Technology Integration

- **Google Products**
    - Google Classroom - Used for daily interactions with the students covering a vast majority of different educational resources (Daily Notes, Exit Tickets, Classroom Polls, Quick Checks, Additional Resources/ Support, Homework, etc.)
    - GAFE (Google Apps For Education) - Using various programs connected with Google to collaborate within the district, co-teachers, grade level partner teacher, and with students to stay connected with the content that is covered within the topic. Used to collect data in real time and see results upon completion of the assignments to allow for 21st century learning.
- **One to One Student's laptop**
    - All students within the West Deptford School District are given a computer, allowing for 21st century learning to occur within every lesson/topic.
- **Virtual Machines**
    - Students will use virtual machines to demonstrate, test, and analyze different cyber attacks.

Differentiated Instruction

Gifted Students (N.J.A.C.6A:8-3.1)

❑ Within each lesson, the Gifted Students are given choice on topic and subject matter allowing them to explore interests appropriate to their abilities, areas of interest and other courses.

English Language Learners (N.J.A.C.6A:15)

❑ Within each lesson, the English Language Learners are given choice of topic and resources so that their materials are within their ability to grasp the language.

❑ All assignments have been created in the student's native language.

❑ Work with ELL Teacher to allow for all assignments to be completed with extra time.

At-Risk Students (N.J.A.C.6A:8-4.3c)

❑ Within each lesson, the at-risk students are given choice of topic and resources so that their materials are within their ability level and high-interest.

Special Education Students (N.J.A.C.6A:8-3.1)

❑ Within each lesson, special education students are given choice of topic and resources so that their materials are within their ability level and high-interest.

❑ All content will be modeled with examples and all essays are built on a step-by-step basis so modifications for assignments in small chunks are met.

All other IEP modifications will be honored (ie. hard copies of notes, directions restated, etc.)

Interdisciplinary Connections

- Computer Science: Cybersecurity is closely related to computer science as it involves the study of algorithms, data structures, programming languages, and network protocols. Understanding the technical aspects of cybersecurity requires knowledge of computer systems, software development, and encryption techniques.

- Mathematics: Mathematics plays a crucial role in cybersecurity. Concepts such as cryptography, probability theory, and discrete mathematics are fundamental to designing secure algorithms and encryption methods. Understanding mathematical concepts helps in analyzing the strength and vulnerabilities of cryptographic systems.

- Psychology: Cybersecurity involves understanding the motivations and behaviors of hackers, as well as the psychology of individuals targeted by cyberattacks. Psychological concepts such as social engineering, human factors in security, and user behavior play a vital role in designing secure systems and raising awareness about cyber threats.

- Law and Ethics: Cybersecurity is closely tied to legal and ethical considerations. Understanding laws and regulations related to data protection, privacy, intellectual property, and cybercrime is crucial for cybersecurity professionals. Ethical considerations, such as responsible disclosure and the ethics of hacking, are also important topics to explore.

- Business and Management: Cybersecurity has become a critical concern for businesses of all sizes. Understanding cybersecurity risks and developing effective strategies to protect organizational assets requires knowledge of business management principles, risk assessment, and incident response planning. It also involves considering the economic impact of cyber threats on businesses.

- Sociology: Cybersecurity is not solely a technical issue but also a sociological one. Analyzing the societal impact of cyber threats, studying cybercrime patterns, and understanding the social dynamics of online communities are essential for addressing cybersecurity challenges effectively. Sociological perspectives also shed light on issues related to privacy, surveillance, and trust in the digital world.

- Communication Studies: Effective communication is crucial in cybersecurity. Being able to communicate complex technical concepts, risks, and mitigation strategies to both technical and non-technical stakeholders is essential. Studying communication theories, rhetoric, and persuasive techniques helps cybersecurity professionals convey their message clearly and influence behavior change.

- Economics: Cybersecurity has economic implications for individuals, organizations, and society as a whole. Analyzing the cost of cyberattacks, evaluating the return on investment for cybersecurity measures, and understanding the economic incentives behind cybercrime provide valuable insights for designing effective cybersecurity strategies.

- Political Science: Cybersecurity intersects with political science as it involves national security, cyber warfare, and international cooperation on cybersecurity issues. Studying international relations, government policies, and the role of state actors in cyber conflicts helps in understanding the broader context of cybersecurity challenges.

- Education: Cybersecurity education and awareness are crucial for building a cyber-resilient society. Incorporating educational theories, instructional design, and pedagogical strategies into cybersecurity training programs helps in effectively teaching individuals to protect themselves and their organizations from cyber threats.

Learning Plan / Pacing Guide

Course Notes:
• 1 day is ~ a 42-45 minute lesson that meets 5 days per week
• Lessons have several types of learning outside of lecture. These abbreviations are used as a reference:
(G) Group activity) (L) Lab online (A) Activity

3.1 Securing the System – 7 days
1. Define Vulnerability and Exploit – use Darknet Diaries podcast (abbreviated) for story on these topics.
2. Examine how the Common Vulnerability and Exposure database can be used as a research tool.
3. Review and apply the recommended Best Practices configurations for typical PCs.
Activities: (A) CVE Named Vulnerabilities, (L) MBSA Vulnerability Scan, (A) Bingo Securing the System, (A) CyberPatriot Demo system.

3.2 Threat Modeling & IOT – 2 days
1. Understand Threat Modeling to determine what risk you are willing to take and what effort you are willing to put in to secure against threats.
2. Examine vulnerabilities of home Internet of Things (IOT) – Smart devices such as voice assistants, baby monitors, home routers, etc.
Activities: (G) Home IOT SPOONS Game (A) My IOT Threat Model worksheet

Unit 4: Cryptography and Linux

Content Area: **Applied Tech**
Course(s): **Generic Course**
Time Period: **Marking Period 2**
Length: **5 weeks**
Status: **Published**

Standards

Life Literacies and Key Skills

TECH.9.4.12.DC.3	Evaluate the social and economic implications of privacy in the context of safety, law, or ethics (e.g., 6.3.12.HistoryCA.1).
TECH.9.4.12.DC.5	Debate laws and regulations that impact the development and use of software.
TECH.9.4.12.TL.1	Assess digital tools based on features such as accessibility options, capacities, and utility for accomplishing a specified task (e.g., W.11-12.6.).

Computer Science Standards

CS.9-12.8.1.12.CS.1	Describe ways in which integrated systems hide underlying implementation details to simplify user experiences.
CS.9-12.8.1.12.CS.2	Model interactions between application software, system software, and hardware.
CS.9-12.8.1.12.DA.1	Create interactive data visualizations using software tools to help others better understand real world phenomena, including climate change.
CS.9-12.8.1.12.DA.2	Describe the trade-offs in how and where data is organized and stored.
CS.9-12.8.1.12.DA.3	Translate between decimal numbers and binary numbers.
CS.9-12.8.1.12.DA.4	Explain the relationship between binary numbers and the storage and use of data in a computing device.
CS.9-12.8.1.12.NI.2	Evaluate security measures to address various common security threats.
CS.9-12.8.1.12.NI.3	Explain how the needs of users and the sensitivity of data determine the level of security implemented.

Transfer Goals and Career Ready Practices

Transfer Goals

Students will be able to independently use their learning to use cryptography in a real-world situation and use basic terminal commands in Windows and Linux.

Concepts

Essential Questions

- What is the difference between encoding and encryption?
- What is cryptography and steganography?
- What is the difference between privacy and security?
- Why would someone use Linux instead of Windows (and vice versa)?

Understandings

Students will understand that...

- Everything on a computer is represented in bits.
- Capture the Flag challenges are an important way for cybersecurity experts to hone their skills.
- Linux is an operating system, similar to Windows.
- The debate between privacy and security does not have a clear answer.

Critical Knowledge and Skills

Knowledge

Students will know:

• Transistors
• Bit
• Byte
• Binary Number System
• Machine language
• Computer language
• Compiler
• ASCII
• Decimal
• Hexadecimal
• Encoding
• Hashing
• Obfuscation

• Exfiltration

• Cryptography
• Algorithm (aka Cipher)
• Plaintext
• Ciphertext
• Cryptanalysis
• Substitution
• Monoalphabetic ciphers
• Transposition
• Shift cipher
• Key
• Frequency analysis
• Polyalphabetic cipher
• OTP = One-Time Pad
• Steganography
• Binwalk tool

• Paths – Absolute
• Paths – Relative
• Sudo
• Shell
• Script

Skills

Students will be able to:

• Understand that computer language is based on electrical signals called binary code.
• Apply binary math to explore how electrical bits are translated into human language.

• Examine cryptography vocabulary terms and methods of encryption
• Identify cryptographic algorithms and define how they can be used to help improve security

• Review the basic CLI commands for file access and manipulation for Linux (covered in Unit 1.3)
• Apply advanced Linux CLI commands.

• Use news resources to analyze controversies, select and evaluate evidence, construct and refute arguments.

Assessment and Resources

Primary Resources

Intro to Cybersecurity

hosted by cyber.org

available online at https://cyber.instructure.com/courses/243

Supplementary Resources

- cyber.org Cyber Range
- NJ Brookdale CC Cyber Range
- CyberStart America

School Summative Assessment Plan

- Unit Assessment
- Unit Labs
- Unit Project

School Formative Assessment Plan (Other Evidence)

- Guided Notes
- Lesson Activities
- Worksheets

Technology Integration and Differentiated Instruction

Technology Integration

- **Google Products**
    - Google Classroom - Used for daily interactions with the students covering a vast majority of different educational resources (Daily Notes, Exit Tickets, Classroom Polls, Quick Checks, Additional Resources/ Support, Homework, etc.)
    - GAFE (Google Apps For Education) - Using various programs connected with Google to collaborate within the district, co-teachers, grade level partner teacher, and with students to stay connected with the content that is covered within the topic. Used to collect data in real time and see results upon completion of the assignments to allow for 21st century learning.

- **One to One Student's laptop**
    - All students within the West Deptford School District are given a computer, allowing for 21st century learning to occur within every lesson/topic.

- **Virtual Machines**
    - Students will use virtual machines to demonstrate, test, and analyze different cyber attacks.

Differentiated Instruction

Gifted Students (N.J.A.C.6A:8-3.1)

❑ Within each lesson, the Gifted Students are given choice on topic and subject matter allowing them to explore interests appropriate to their abilities, areas of interest and other courses.

English Language Learners (N.J.A.C.6A:15)

❑ Within each lesson, the English Language Learners are given choice of topic and resources so that their materials are within their ability to grasp the language.

❑ All assignments have been created in the student's native language.

❑ Work with ELL Teacher to allow for all assignments to be completed with extra time.

At-Risk Students (N.J.A.C.6A:8-4.3c)

❑ Within each lesson, the at-risk students are given choice of topic and resources so that their materials are within their ability level and high-interest.

Special Education Students (N.J.A.C.6A:8-3.1)

❑ Within each lesson, special education students are given choice of topic and resources so that their materials are within their ability level and high-interest.

❑ All content will be modeled with examples and all essays are built on a step-by-step basis so

modifications for assignments in small chunks are met.

All other IEP modifications will be honored (ie. hard copies of notes, directions restated, etc.)

Interdisciplinary Connections

- Computer Science: Cybersecurity is closely related to computer science as it involves the study of algorithms, data structures, programming languages, and network protocols. Understanding the technical aspects of cybersecurity requires knowledge of computer systems, software development, and encryption techniques.

- Mathematics: Mathematics plays a crucial role in cybersecurity. Concepts such as cryptography, probability theory, and discrete mathematics are fundamental to designing secure algorithms and encryption methods. Understanding mathematical concepts helps in analyzing the strength and vulnerabilities of cryptographic systems.

- Psychology: Cybersecurity involves understanding the motivations and behaviors of hackers, as well as the psychology of individuals targeted by cyberattacks. Psychological concepts such as social engineering, human factors in security, and user behavior play a vital role in designing secure systems and raising awareness about cyber threats.

- Law and Ethics: Cybersecurity is closely tied to legal and ethical considerations. Understanding laws and regulations related to data protection, privacy, intellectual property, and cybercrime is crucial for cybersecurity professionals. Ethical considerations, such as responsible disclosure and the ethics of hacking, are also important topics to explore.

- Business and Management: Cybersecurity has become a critical concern for businesses of all sizes. Understanding cybersecurity risks and developing effective strategies to protect organizational assets requires knowledge of business management principles, risk assessment, and incident response planning. It also involves considering the economic impact of cyber threats on businesses.

- Sociology: Cybersecurity is not solely a technical issue but also a sociological one. Analyzing the societal impact of cyber threats, studying cybercrime patterns, and understanding the social dynamics of online communities are essential for addressing cybersecurity challenges effectively. Sociological perspectives also shed light on issues related to privacy, surveillance, and trust in the digital world.

- Communication Studies: Effective communication is crucial in cybersecurity. Being able to communicate complex technical concepts, risks, and mitigation strategies to both technical and non-technical stakeholders is essential. Studying communication theories, rhetoric, and persuasive techniques helps cybersecurity professionals convey their message clearly and influence behavior change.

- Economics: Cybersecurity has economic implications for individuals, organizations, and society as a whole. Analyzing the cost of cyberattacks, evaluating the return on investment for cybersecurity measures, and understanding the economic incentives behind cybercrime provide valuable insights for designing effective cybersecurity strategies.

- Political Science: Cybersecurity intersects with political science as it involves national security, cyber warfare, and international cooperation on cybersecurity issues. Studying international relations,

government policies, and the role of state actors in cyber conflicts helps in understanding the broader context of cybersecurity challenges.

- Education: Cybersecurity education and awareness are crucial for building a cyber-resilient society. Incorporating educational theories, instructional design, and pedagogical strategies into cybersecurity training programs helps in effectively teaching individuals to protect themselves and their organizations from cyber threats.

Learning Plan / Pacing Guide

Course Notes:
• 1 day is ~ a 42-45 minute lesson that meets 5 days per week
• Lessons have several types of learning outside of lecture. These abbreviations are used as a reference: (G) Group activity) (L) Lab online (A) Activity

---

4.1 Bits, Binary, & Encoding – 7 days
1. Define bits, bytes and binary number system as computer language
2. Define hexadecimal numbers, use in computing
3. Define encoding and differences from encryption
4. Introduce using Capture The Flag challenges for practice.
Activities: (L) online Binary game; (A) Convert between Decimal, Binary and Hex numbers; (L) Decoding with CTF challenges. Resource set of alternate ways to learn binary and hex numbers.

4.2 Basic Cryptography Concepts – 6 days
1. Define terminology for cryptography
2. Define key methods of encryption and examine classic algorithms including Caesar, Transposition and Vigenere
3. Define Steganography and tools to find hidden data – hex editor, steghide, Cyberchef, Exifdata, binwalk
Activities: (G) Breaking Ciphers, (A) Vigenere Try It (G) Scavenger Hunt, (L) Steganography CTF

4.3 Advanced Linux CLI – 5 days
1. Review basic terminal commands in Linux and Windows
2. Advanced terminal commands in Linux
3. Create simple bash scripts that demo cybersecurity impact on device
Activities: (L) Terminus game part 2, (L) Try It follow along with PPT, (L) Searching with Grep (L) Shell scripting in Linux

---

4.4 Privacy vs Security – 4 days
1. Define difference between privacy and security
2. Review facts of case where FBI demanded access to encrypted iPhone
3. Watch excerpts from debate on the privacy vs security concepts – Fareed Zakaria (NY Times) and Edward Snowden (NSA hacker)

4. Student teams debate same topic: Government should have lawful access to any encrypted message or device
Activities: (G) Class debate

Unit 5: Devices and Networks

Content Area: **Applied Tech**
Course(s): **Generic Course**
Time Period: **Marking Period 2**
Length: **3 weeks**
Status: **Published**

Standards

Life Literacies and Key Skills

TECH.9.4.12.DC.5	Debate laws and regulations that impact the development and use of software.
TECH.9.4.12.TL.1	Assess digital tools based on features such as accessibility options, capacities, and utility for accomplishing a specified task (e.g., W.11-12.6.).

Computer Science Standards

CS.9-12.8.1.12.CS.1	Describe ways in which integrated systems hide underlying implementation details to simplify user experiences.
CS.9-12.8.1.12.CS.2	Model interactions between application software, system software, and hardware.
CS.9-12.8.1.12.CS.3	Compare the functions of application software, system software, and hardware.
CS.9-12.8.1.12.NI.1	Evaluate the scalability and reliability of networks, by describing the relationship between routers, switches, servers, topology, and addressing.
CS.9-12.8.1.12.NI.2	Evaluate security measures to address various common security threats.
CS.9-12.8.1.12.NI.4	Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.

Transfer Goals and Career Ready Practices

Transfer Goals

Students will be able to independently use their learning to create networks and establish protocols for their use and maintenance.

Concepts

Essential Questions

- What are the key physical components of a computing device?
- What different devices make up a computing network?
- How is information shared on the Internet?

Understandings

Students will understand that...

- Packet switching is a common network method of communication.
- Network naming has changed as the Internet has expanded.
- Network packet traffic gives a lot of information about network usage and security.
- Computing devices share a number of physical components.

Critical Knowledge and Skills

Knowledge

Students will know:

• Processor (aka Central Processing Unit or CPU)
• Memory
• Motherboard
• Hard Drive
• Graphics card
• Network Interface Card
• Input
• Storage
• Output
• RAM = Random Access Memory
• Machine Code
• Compiler
• Computer Language

• Hosts
• Media
• Network Devices
• Peripherals
• Services
• Interfaces
• MAC address
• IP Address

• Address Resolution Protocol (ARP)
• Local Area Network (LAN)
• Wide Area Network (WAN)
• Hub
• Switch
• Wireless Access Point

• Networks
• Protocol
• Reliability
• Network Packet Analyzer / Packet sniffer
• Packet List
• Packet Details
• Packet Bytes
• Pcap
• Follow TCP Stream
• ifconfig
• ping
• ssh
• netcat

Skills

Students will be able to:

• Identify students' prior knowledge of PC components
• Identify the 4 basic functions of computer Input, Storage, Processing and Output
• Understand how 3 key components process data – Motherboard, CPU, and Memory.
• Examine instances of attacks on the key PC components

• Define difference between LAN and WAN
• Identify characteristics of central connection devices

• Understand analog method of message delivery as a single communication
• Devise a delivery method for messages that are broken up into packets

Assessment and Resources

Primary Resources

Intro to Cybersecurity

hosted by cyber.org

available online at https://cyber.instructure.com/courses/243

Supplementary Resources

- cyber.org Cyber Range
- NJ Brookdale CC Cyber Range
- CyberStart America

School Summative Assessment Plan

- Unit Assessment
- Unit Labs
- Unit Project

School Formative Assessment Plan (Other Evidence)

- Guided Notes
- Lesson Activities
- Worksheets

Technology Integration and Differentiated Instruction

Technology Integration

- **Google Products**
    - Google Classroom - Used for daily interactions with the students covering a vast majority of different educational resources (Daily Notes, Exit Tickets, Classroom Polls, Quick Checks, Additional Resources/ Support, Homework, etc.)
    - GAFE (Google Apps For Education) - Using various programs connected with Google to collaborate within the district, co-teachers, grade level partner teacher, and with students to stay connected with the content that is covered within the topic. Used to collect data in real time and see results upon completion of the assignments to allow for 21st century learning.

- **One to One Student's laptop**

- All students within the West Deptford School District are given a computer, allowing for 21st century learning to occur within every lesson/topic.

● **Virtual Machines**

- Students will use virtual machines to demonstrate, test, and analyze different cyber attacks.

Differentiated Instruction

Gifted Students (N.J.A.C.6A:8-3.1)

❑ Within each lesson, the Gifted Students are given choice on topic and subject matter allowing them to explore interests appropriate to their abilities, areas of interest and other courses.

English Language Learners (N.J.A.C.6A:15)

❑ Within each lesson, the English Language Learners are given choice of topic and resources so that their materials are within their ability to grasp the language.

❑ All assignments have been created in the student's native language.

❑ Work with ELL Teacher to allow for all assignments to be completed with extra time.

At-Risk Students (N.J.A.C.6A:8-4.3c)

❑ Within each lesson, the at-risk students are given choice of topic and resources so that their materials are within their ability level and high-interest.

Special Education Students (N.J.A.C.6A:8-3.1)

❑ Within each lesson, special education students are given choice of topic and resources so that their materials are within their ability level and high-interest.

❑ All content will be modeled with examples and all essays are built on a step-by-step basis so modifications for assignments in small chunks are met.

All other IEP modifications will be honored (ie. hard copies of notes, directions restated, etc.)

Interdisciplinary Connections

- Computer Science: Cybersecurity is closely related to computer science as it involves the study of algorithms, data structures, programming languages, and network protocols. Understanding the technical aspects of cybersecurity requires knowledge of computer systems, software development, and encryption techniques.

- Mathematics: Mathematics plays a crucial role in cybersecurity. Concepts such as cryptography, probability theory, and discrete mathematics are fundamental to designing secure algorithms and encryption methods. Understanding mathematical concepts helps in analyzing the strength and vulnerabilities of cryptographic systems.

- Psychology: Cybersecurity involves understanding the motivations and behaviors of hackers, as well as the psychology of individuals targeted by cyberattacks. Psychological concepts such as social engineering, human factors in security, and user behavior play a vital role in designing secure systems and raising awareness about cyber threats.

- Law and Ethics: Cybersecurity is closely tied to legal and ethical considerations. Understanding laws and regulations related to data protection, privacy, intellectual property, and cybercrime is crucial for cybersecurity professionals. Ethical considerations, such as responsible disclosure and the ethics of hacking, are also important topics to explore.

- Business and Management: Cybersecurity has become a critical concern for businesses of all sizes. Understanding cybersecurity risks and developing effective strategies to protect organizational assets requires knowledge of business management principles, risk assessment, and incident response planning. It also involves considering the economic impact of cyber threats on businesses.

- Sociology: Cybersecurity is not solely a technical issue but also a sociological one. Analyzing the societal impact of cyber threats, studying cybercrime patterns, and understanding the social dynamics of online communities are essential for addressing cybersecurity challenges effectively. Sociological perspectives also shed light on issues related to privacy, surveillance, and trust in the digital world.

- Communication Studies: Effective communication is crucial in cybersecurity. Being able to communicate complex technical concepts, risks, and mitigation strategies to both technical and non-technical stakeholders is essential. Studying communication theories, rhetoric, and persuasive techniques helps cybersecurity professionals convey their message clearly and influence behavior change.

- Economics: Cybersecurity has economic implications for individuals, organizations, and society as a whole. Analyzing the cost of cyberattacks, evaluating the return on investment for cybersecurity measures, and understanding the economic incentives behind cybercrime provide valuable insights for designing effective cybersecurity strategies.

- Political Science: Cybersecurity intersects with political science as it involves national security, cyber warfare, and international cooperation on cybersecurity issues. Studying international relations, government policies, and the role of state actors in cyber conflicts helps in understanding the broader

context of cybersecurity challenges.

- Education: Cybersecurity education and awareness are crucial for building a cyber-resilient society. Incorporating educational theories, instructional design, and pedagogical strategies into cybersecurity training programs helps in effectively teaching individuals to protect themselves and their organizations from cyber threats.

Learning Plan / Pacing Guide

Course Notes:
• 1 day is ~ a 42-45 minute lesson that meets 5 days per week
• Lessons have several types of learning outside of lecture. These abbreviations are used as a reference: (G) Group activity) (L) Lab online (A) Activity

---

5.1 Computer Components – 2 days
1. Device key components – Input, Memory, CPU, Output plus Motherboard. What can go wrong?
Activities: (L) Virtual Desktop Build a PC.

5.2 Networking Fundamentals – 6 days
1. Networking devices and topologies – WAN, LAN, routers, switches.
2. Define network naming – Mac vs IP addresses (basic formatting of IP addressing and subnetting) , IPv4 & IPv6
Activities: (L) ARP with Wireshark, (A) Network Puzzles (L) CS Interactives: Pizza Party (review of Mac/IP addressing).

5.3 Protocols and Packets & Getting to the Internet – 4 days
1. Define packet switching as network method of communication.
2. Define protocols, TCP/IP Suite, ports, 3-way handshake
3. Analyze network packet traffic
Activities: (G) Mobster Net (L) Wireshark Packet Analysis

Unit 6: Final Projects

Content Area: **Applied Tech**
Course(s): **Generic Course**
Time Period: **Marking Period 2**
Length: **2 weeks**
Status: **Published**

Standards

Life Literacies and Key Skills

TECH.9.4.12.CI.1	Demonstrate the ability to reflect, analyze, and use creative skills and ideas (e.g., 1.1.12prof.CR3a).
TECH.9.4.12.CI.3	Investigate new challenges and opportunities for personal growth, advancement, and transition (e.g., 2.1.12.PGD.1).
TECH.9.4.12.TL.3	Analyze the effectiveness of the process and quality of collaborative environments.
TECH.9.4.12.TL.4	Collaborate in online learning communities or social networks or virtual worlds to analyze and propose a resolution to a real-world problem (e.g., 7.1.AL.IPERS.6).

Computer Science Standards

CS.9-12.8.1.12.IC.1	Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.
CS.9-12.8.1.12.IC.2	Test and refine computational artifacts to reduce bias and equity deficits.
CS.9-12.8.1.12.IC.3	Predict the potential impacts and implications of emerging technologies on larger social, economic, and political structures, using evidence from credible sources.

Transfer Goals and Career Ready Practices

Transfer Goals

Students will be able to independently use their learning to complete a final project that is meaningful to them.

Concepts

Essential Questions

- What are some ways in which cybersecurity technology can make an impact?

Understandings

Students will understand that...

- Biometric technology can be an important part of an authentication process.
- Users need to be made aware of methods of social engineering.
- OS hardening is a process which requires benchmarking.
- Cybersecurity has a great impact in our world today.

Critical Knowledge and Skills

Knowledge

Students will know:

• Biometric Technology

• Authentication

• Social Engineering

• PSA

• Benchmark Selections

• OS Hardening

Skills

Students will be able to:

• Explore how technology/cybersecurity can be used to make an impact for social good.

• Investigate a cybersecurity aspect that has interested them over the past semester.

• Present their findings to the class.

• Work collaboratively.

Assessment and Resources

Primary Resources

Intro to Cybersecurity

hosted by cyber.org

available online at https://cyber.instructure.com/courses/243

Supplementary Resources

- cyber.org Cyber Range
- NJ Brookdale CC Cyber Range
- CyberStart America

School Summative Assessment Plan

- Unit Project

School Formative Assessment Plan (Other Evidence)

- Lesson Activities
- Reflections

Technology Integration and Differentiated Instruction

Technology Integration

- **Google Products**
    - Google Classroom - Used for daily interactions with the students covering a vast majority of different educational resources (Daily Notes, Exit Tickets, Classroom Polls, Quick Checks, Additional Resources/ Support, Homework, etc.)
    - GAFE (Google Apps For Education) - Using various programs connected with Google to collaborate within the district, co-teachers, grade level partner teacher, and with students to stay connected with the content that is covered within the topic. Used to collect data in real time and see results upon completion of the assignments to allow for 21st century learning.
- **One to One Student's laptop**
    - All students within the West Deptford School District are given a computer, allowing for 21st century learning to occur within every lesson/topic.
- **Virtual Machines**
    - Students will use virtual machines to demonstrate, test, and analyze different cyber attacks.

Differentiated Instruction

Gifted Students (N.J.A.C.6A:8-3.1)

❑ Within each lesson, the Gifted Students are given choice on topic and subject matter allowing them to explore interests appropriate to their abilities, areas of interest and other courses.

English Language Learners (N.J.A.C.6A:15)

❑ Within each lesson, the English Language Learners are given choice of topic and resources so that their materials are within their ability to grasp the language.

❑ All assignments have been created in the student's native language.

❑ Work with ELL Teacher to allow for all assignments to be completed with extra time.

At-Risk Students (N.J.A.C.6A:8-4.3c)

❑ Within each lesson, the at-risk students are given choice of topic and resources so that their materials are within their ability level and high-interest.

Special Education Students (N.J.A.C.6A:8-3.1)

❑ Within each lesson, special education students are given choice of topic and resources so that their materials are within their ability level and high-interest.

❑ All content will be modeled with examples and all essays are built on a step-by-step basis so modifications for assignments in small chunks are met.

All other IEP modifications will be honored (ie. hard copies of notes, directions restated, etc.)

Interdisciplinary Connections

- Computer Science: Cybersecurity is closely related to computer science as it involves the study of algorithms, data structures, programming languages, and network protocols. Understanding the technical aspects of cybersecurity requires knowledge of computer systems, software development, and encryption techniques.

- Mathematics: Mathematics plays a crucial role in cybersecurity. Concepts such as cryptography, probability theory, and discrete mathematics are fundamental to designing secure algorithms and encryption methods. Understanding mathematical concepts helps in analyzing the strength and vulnerabilities of cryptographic systems.

- Psychology: Cybersecurity involves understanding the motivations and behaviors of hackers, as well as the psychology of individuals targeted by cyberattacks. Psychological concepts such as social engineering, human factors in security, and user behavior play a vital role in designing secure systems and raising awareness about cyber threats.

- Law and Ethics: Cybersecurity is closely tied to legal and ethical considerations. Understanding laws and regulations related to data protection, privacy, intellectual property, and cybercrime is crucial for cybersecurity professionals. Ethical considerations, such as responsible disclosure and the ethics of hacking, are also important topics to explore.

- Business and Management: Cybersecurity has become a critical concern for businesses of all sizes. Understanding cybersecurity risks and developing effective strategies to protect organizational assets requires knowledge of business management principles, risk assessment, and incident response planning. It also involves considering the economic impact of cyber threats on businesses.

- Sociology: Cybersecurity is not solely a technical issue but also a sociological one. Analyzing the societal impact of cyber threats, studying cybercrime patterns, and understanding the social dynamics of online communities are essential for addressing cybersecurity challenges effectively. Sociological perspectives also shed light on issues related to privacy, surveillance, and trust in the digital world.

- Communication Studies: Effective communication is crucial in cybersecurity. Being able to communicate complex technical concepts, risks, and mitigation strategies to both technical and non-technical stakeholders is essential. Studying communication theories, rhetoric, and persuasive

techniques helps cybersecurity professionals convey their message clearly and influence behavior change.

- Economics: Cybersecurity has economic implications for individuals, organizations, and society as a whole. Analyzing the cost of cyberattacks, evaluating the return on investment for cybersecurity measures, and understanding the economic incentives behind cybercrime provide valuable insights for designing effective cybersecurity strategies.

- Political Science: Cybersecurity intersects with political science as it involves national security, cyber warfare, and international cooperation on cybersecurity issues. Studying international relations, government policies, and the role of state actors in cyber conflicts helps in understanding the broader context of cybersecurity challenges.

- Education: Cybersecurity education and awareness are crucial for building a cyber-resilient society. Incorporating educational theories, instructional design, and pedagogical strategies into cybersecurity training programs helps in effectively teaching individuals to protect themselves and their organizations from cyber threats.

Learning Plan / Pacing Guide

Students will choose from the following projects:
1. Which Authentication – Sales Pitch of Biometric Technology
2. Social Engineering PSA video
3. Benchmark Selections for OS Hardening
4. Making an Impact with Cybersecurity Technology

Students may work with a partner. Rubrics will be provided for each project and presented during the exam period.