Cybersecurity II

Level: 3
Career Cluster: Digital Technology
Program: Information Technology
Pathway(s): Networking Systems and Security

Course Catalog Description

Course that builds on foundational cybersecurity concepts by introducing students to advanced topics in threat analysis, system protection, and secure network practices. Students apply knowledge of malware, vulnerabilities, cryptography, wireless security, and risk management to analyze and respond to cybersecurity challenges while developing problem-solving, communication, and professional skills in real-world security scenarios.

Summary

Course that builds on foundational cybersecurity concepts by developing students' advanced knowledge of system protection, threat analysis, and secure network practices. Students examine legal and ethical considerations, analyze cybercrime cases, and apply responsible decision-making when handling digital evidence and organizational security challenges. Through hands-on learning and scenario-based activities, students investigate malware behavior, identify threats and vulnerabilities, and apply strategies for detection, mitigation, and response. The course emphasizes cryptography, wireless security, and risk management while developing skills in analyzing attacks, securing systems, and designing policy-based solutions to protect data and infrastructure. Students also engage in security monitoring and incident response processes, using evidence and technical reasoning to document findings and recommend solutions.

Notes

The updated course reflects a significant evolution from a primarily topic-driven, concept-based outline to a more structured, application-focused program that integrates advanced technical skills with professional practice. The original course emphasized key cybersecurity areas such as legal issues, malware, threats and vulnerabilities, cryptology, wireless security, and organizational security as individual content areas with limited progression. In contrast, the revised course organizes these topics into clearly defined learning sections with explicit objectives and expanded student outcomes, creating a more intentional sequence from foundational analysis to applied problem solving. The updated version strengthens depth by incorporating detailed focus on incident response, security monitoring, and risk management strategies, expanding beyond identification of threats to include evaluation and decision-making processes. It also enhances practical application through scenario-based learning and emphasizes documentation, analysis, and justification of cybersecurity decisions.

Student Learning Outcomes

1. Career Exploration and Postsecondary Opportunities

Objective: *Students will analyze career pathways in information technology, exploring industry roles, workplace expectations, required education, certifications, professional organizations, and postsecondary opportunities available in Colorado in order to make informed academic and career decisions.*

1) Identify employment opportunities in various fields with a focus in the area of information technology
    a. Recognize the work typically performed, tools and technology used, and nature of work environments
    b. Identify potential certifications within the careers
    c. Find membership organizations associated with the careers
    d. Understand the necessary education associated within the careers
2) Define professionalism within the context of information technology
    a. Criticism and evaluation
    b. Presentation
    c. Assessment
3) Recognize laws, regulations, and ethics significant to the fields of information technology
4) Identify postsecondary opportunities offered in the state of Colorado
    a. Technical college, community college, 4-year institutions
    b. Certificates, associates, bachelor, and advanced degree opportunities

2. Cybersecurity Law, Ethics, and Digital Responsibility

Objective: *Students will analyze legal, ethical, and professional responsibilities in cybersecurity in order to make informed decisions about digital conduct, evidence handling, and organizational compliance.*

5) Analyze current legislation and regulations related to computer crime and cybersecurity
6) Investigate legal cases involving cybercrime and summarize the issues and outcomes
7) Explain ethical responsibilities related to cybersecurity practice and digital evidence
8) Differentiate between legal, ethical, and organizational responses to cyber incidents
9) Evaluate methods used to collect and preserve digital evidence
10) Justify responsible decision-making when responding to security incidents
11) Assess the impact of unethical behavior on individuals, organizations, and digital systems

3. Malware Analysis and Defensive Response

Objective: *Students will examine malware behavior and apply defensive strategies in order to reduce system risk and improve incident response.*

12) Identify common forms of malware, including viruses, worms, trojans, ransomware, and spyware

13) Differentiate among malware behaviors, infection methods, and system impacts
14) Analyze strategies for detecting, containing, and removing malware
15) Explain how BIOS, startup settings, and recovery tools can support malware response
16) Apply safe procedures for handling suspected malware incidents
17) Evaluate defensive tools and techniques used to protect systems from malware
18) Recommend response actions based on the severity and scope of an infection

4. Threats, Vulnerabilities, and Attack Methods

Objective: *Students will evaluate cybersecurity threats and vulnerabilities in order to understand how attacks occur and how systems can be protected.*

19) Differentiate among common attack types that affect systems and networks
20) Explain how threats such as password cracking, unpatched software, reconnaissance, and infiltration create risk
21) Analyze attacks including DoS, DDoS, session hijacking, DNS attacks, switch attacks, and man-in-the-middle attacks
22) Examine web-based attacks such as cross-site scripting and drive-by attacks
23) Interpret how attackers exploit vulnerabilities to gain access or disrupt services
24) Evaluate system weaknesses to determine likely attack paths
25) Recommend mitigation strategies to reduce exposure to threats and vulnerabilities

5. Cryptography and Secure Communication

Objective: *Students will analyze principles of cryptology and apply encryption concepts in order to protect data and support secure communication.*

26) Explain the purpose of cryptography in cybersecurity
27) Differentiate between encryption, hashing, digital signatures, and certificates
28) Analyze cryptographic tools, procedures, and products used to protect information
29) Describe the role of PKI, certificate authorities, and PGP in secure communication
30) Develop a simple public key infrastructure model for a small business or classroom scenario
31) Demonstrate creation of a self-signed certificate for a web server or secure service
32) Evaluate strengths and limitations of cryptographic methods for different security needs

6. Wireless Security and Secure Network Access

Objective: *Students will analyze wireless network risks and apply security techniques in order to improve the protection of wireless communication environments.*

33) Identify common wireless attack methods and explain how they affect network security
34) Differentiate among wireless security protocols including WEP, WPA, and WPA2
35) Evaluate the effectiveness of wireless security protocols in different use cases
36) Demonstrate configuration of wireless security settings using appropriate protocols
37) Analyze how misconfiguration increases wireless network vulnerability

38) Recommend strategies to improve secure wireless access and reduce unauthorized connections
39) Assess wireless environments for weaknesses related to authentication, encryption, and access control

7. Risk Management, Security Analysis, and Contingency Planning

Objective: *Students will apply risk management and security analysis strategies in order to identify concerns, prioritize responses, and support continuity of operations.*

40) Explain the purpose of risk management in cybersecurity
41) Identify assets, threats, vulnerabilities, and possible impacts in a given scenario
42) Analyze risks to determine likelihood and severity
43) Prioritize mitigation strategies based on organizational needs and available resources
44) Develop simple contingency or response plans for security incidents
45) Evaluate how security analysis supports informed decision-making
46) Recommend improvements to risk response and continuity planning practices

8. Organizational Security Policies and Security Awareness

Objective: *Students will evaluate organizational security practices and develop policy-based solutions in order to support safe and effective cybersecurity operations.*

47) Analyze the role of environmental controls in organizational security
48) Explain how policies and procedures support secure operations
49) Collaborate to develop simple security policies for classroom or business scenarios
50) Evaluate the effectiveness of security awareness initiatives in organizations
51) Design basic user awareness guidance related to safe behavior and risk reduction
52) Recommend policy improvements based on identified organizational risks
53) Justify the importance of shared responsibility in maintaining organizational security

9. Security Monitoring, Incident Handling, and Response

Objective: *Students will apply investigation and response procedures in order to analyze incidents, document findings, and support secure recovery practices.*

54) Identify indicators that a cybersecurity incident may have occurred
55) Differentiate among preparation, detection, containment, eradication, recovery, and review stages of incident handling
56) Analyze evidence from logs, alerts, or suspicious behavior to determine possible causes
57) Document incident details using clear and organized technical language
58) Recommend appropriate response actions based on the type and severity of an incident
59) Evaluate the effectiveness of response steps after an incident is resolved
60) Reflect on lessons learned to improve future security practices

10. Work-Based Learning and Professional Practice

Objective: *Students will apply cybersecurity knowledge and professional behaviors in authentic workplace settings in order to strengthen readiness for technical and security-related responsibilities.*

61) Apply cybersecurity concepts during labs, simulations, or scenario-based tasks
62) Demonstrate professionalism, accountability, and responsible conduct when handling sensitive information
63) Communicate technical information clearly to peers, instructors, or stakeholders
64) Document security procedures, findings, and recommendations using professional language
65) Follow established safety, privacy, and acceptable-use expectations in technical environments
66) Evaluate personal work habits and technical growth through reflection
67) Connect classroom cybersecurity practices to workplace expectations and operational needs

11. Leadership and Collaborative Security Operations

Objective: *Students will demonstrate leadership, collaboration, and ethical responsibility in order to contribute effectively to team-based cybersecurity tasks and decision-making.*

68) Collaborate with peers to analyze security issues and propose solutions
69) Demonstrate leadership by organizing tasks, supporting team goals, and contributing informed ideas
70) Practice respectful communication during technical discussions, critiques, and response planning
71) Evaluate team processes and individual contributions using reflection and feedback
72) Defend cybersecurity decisions using evidence, logic, and appropriate terminology
73) Model ethical conduct when addressing shared digital risks and responsibilities
74) Set goals for continued leadership development in technical environments

12. Final Assessment Project

Objective: *Students will design, analyze, document, and present a cybersecurity solution or response plan that demonstrates technical understanding, problem solving, and professional communication.*

75) Analyze a cybersecurity scenario involving legal, technical, and organizational concerns
76) Develop a project that addresses threats, vulnerabilities, risk, and security controls
77) Apply concepts from malware defense, cryptography, wireless security, and policy development
78) Create supporting documentation that explains security decisions and recommended actions
79) Evaluate project effectiveness using established criteria or evidence from testing and analysis

80) Present findings and justify solutions using cybersecurity terminology and technical reasoning
81) Reflect on project outcomes and recommend next steps for improvement or future implementation

13. Career and Technical Student Organizations

Objective: *Using the CTSO Resource Document, chapter activities will provide some of the best opportunities CTSO members will have to learn by doing. A successful program of work creates a positive learning atmosphere in the classroom. CTSO members learn how to accept responsibility, work as a team, manage a budget, and handle success and failure. Per the CTE Admin Handbook, CTSOs are embedded into curriculum.*

Professional Development

Prepare each member for entry into the workforce and provide a foundation for success in a career. Becoming a professional does not stop with acquiring a skill, but involves an increased awareness of the meaning of good citizenship and the importance of labor and management in the world of work.

Community Service

Promote and improve goodwill and understanding among all segments of the community through services donated by CTSO chapters, and to instill in its members a lifetime commitment to community service.

Business and Industry Connections

Increase awareness of quality job practices and attitudes, and increase the opportunities for employer engagement and eventual employment.

Financial Leadership

Plan and participate in activities to allow all members to carry out the chapter's projects. Educate members on their own personal finance for current and future success.

Public Relations

Make the general public aware of the good work that students in career and technical education are doing to better themselves and their community, state, nation, and world.

Social Activities

To increase cooperation in the school and community through activities that allow CTSO members to get to know each other in something other than a business or classroom setting.

Academic Standards Alignment

Colorado CTE courses are required to integrate academic and essential skills into course content. The following academic standards have been identified as aligned to this course and should be integrated throughout instruction.

CO CTE Academic Standards Resources (Rubrics, integration strategies, etc)
CDE Colorado Academic Standards Online (Online standards lookup tool)

Note: Mathematics and Science standards will be added in the future. Visit the Colorado Academic Standards page for the most current version.

Reading, Writing and Communicating Crosswalk

Course: Cybersecurity II
Colorado Academic Standards – Reading, Writing, and Communicating

Standard	Prepared Graduate Competency	Description	Course Evidence / Alignment
Standard 1: Oral Expression and Listening	Prepared Graduate 1 – Collaboration	Collaborate effectively as group members or leaders	Students work collaboratively to analyze security threats, develop organizational security policies, and plan risk mitigation strategies.
Standard 1: Oral Expression and Listening	Prepared Graduate 2 – Oral Presentations	Deliver effective oral presentations	Students explain cybersecurity threats, vulnerabilities, cryptographic techniques, and security recommendations to classmates or instructors.
Standard 2: Reading for All Purposes	Prepared Graduate 4 – Informational Texts	Read a wide range of informational texts	Students read and interpret technical documentation, cybersecurity standards, legislation, case studies, and threat analysis reports.
Standard 2:	Prepared	Understand how language	Students use

Reading for All Purposes	Graduate 5 – Language in Context	functions in different contexts	discipline-specific cybersecurity terminology and adjust communication when addressing technical peers versus non-technical stakeholders.
Standard 3: Writing and Composition	Prepared Graduate 7 – Informational Writing	Craft informational/explanatory texts	Students produce written analyses, reports, incident documentation, and security policy explanations.
Standard 3: Writing and Composition	Prepared Graduate 9 – Writing Process	Demonstrate mastery of the writing process	Students revise and polish security documentation and analytical writing to ensure accuracy, clarity, and professional quality.
Standard 4: Research Inquiry and Design	Prepared Graduate 10 – Research and Ethics	Gather and ethically use information	Students research cybersecurity threats, legal cases, standards, and technologies, evaluate source credibility, and apply information ethically and responsibly.

Free Resource Links

1. Career Exploration and Postsecondary Opportunities

- CompTIA Cybersecurity Careers (certifications, career pathways, cybersecurity roles)
  https://www.comptia.org/content/it-careers-path-roadmap
- O NET Online Cybersecurity Careers (job roles, skills, work environments)
  https://www.onetonline.org
- CareerOneStop IT Careers (career exploration, job outlook, education pathways)
  https://www.careeronestop.org/ExploreCareers/explore-careers.aspx
- Colorado Community Colleges (postsecondary programs, certificates, degrees)
  https://cccs.edu

2. Cybersecurity Law, Ethics, and Digital Responsibility

- Department of Justice Cybercrime Resources (laws, digital evidence, cybercrime cases)
  https://www.justice.gov/criminal-ccips
- Electronic Frontier Foundation (digital rights, privacy, ethics)
  https://www.eff.org
- NIST Cybersecurity Framework (policies, ethics, security standards)
  https://www.nist.gov/cyberframework
- Cybersecurity and Infrastructure Security Agency (legal guidance, cyber awareness)
  https://www.cisa.gov

3. Malware Analysis and Defensive Response

- Kaspersky Resource Center (malware types, detection, removal strategies)
  https://www.kaspersky.com/resource-center
- Cisco Malware Defense (malware protection, detection tools, prevention)
  https://www.cisco.com
- Microsoft Security Intelligence (malware analysis, threats, response)
  https://www.microsoft.com/en-us/security
- Avast Threat Labs (malware behavior, security tools, defense)
  https://www.avast.com/threat-labs

4. Threats, Vulnerabilities, and Attack Methods

- OWASP Top Ten (web vulnerabilities, attack methods, mitigation)
  https://owasp.org/www-project-top-ten
- Cloudflare Learning Security Attacks (DDoS, spoofing, attack methods)
  https://www.cloudflare.com/learning/security
- MITRE ATT&CK Framework (threat tactics, attack techniques, vulnerabilities)
  https://attack.mitre.org
- Cisco Threat Intelligence (cyber threats, vulnerabilities, analysis)
  https://www.cisco.com

5. Cryptography and Secure Communication

- Khan Academy Cryptography (encryption, hashing, secure communication) https://www.khanacademy.org/computing/computer-science/cryptography
- IBM Cryptography Overview (encryption, PKI, digital security) https://www.ibm.com/topics/cryptography
- DigiCert Learning Center (certificates, PKI, authentication) https://www.digicert.com/resources
- GeeksforGeeks Cryptography (encryption, hashing, digital signatures) https://www.geeksforgeeks.org/cryptography-and-network-security/

6. Wireless Security and Secure Network Access

- Cisco Wireless Security (WPA, encryption, wireless protection) https://www.cisco.com
- Intel Wireless Networking Security (WiFi security, protocols, protection) https://www.intel.com
- CWNP Wireless Security Basics (wireless vulnerabilities, protection methods) https://www.cwnp.com
- SANS Wireless Security Guide (wireless risks, mitigation strategies) https://www.sans.org

7. Risk Management Security Analysis and Contingency Planning

- NIST Risk Management Framework (risk analysis, mitigation, security planning) https://www.nist.gov
- ISO Information Security Standards (risk management, compliance, frameworks) https://www.iso.org
- CISA Cyber Risk Management (risk assessment, contingency planning) https://www.cisa.gov
- ISACA Risk Management Resources (security risk analysis, governance) https://www.isaca.org

8. Organizational Security Policies and Security Awareness

- SANS Security Awareness (training, awareness programs, policy development) https://www.sans.org/security-awareness-training
- NIST Security Policies Guide (organizational policies, governance) https://www.nist.gov
- Cybersecurity Guide Policy Resources (security policies, best practices) https://www.cybersecurityguide.org
- CISA Security Awareness (user training, organizational security practices) https://www.cisa.gov

9. Security Monitoring Incident Handling and Response

- SANS Incident Response (incident handling, response lifecycle) https://www.sans.org
- NIST Incident Response Guide (incident detection, containment, recovery) https://nvlpubs.nist.gov

- IBM Incident Response (security monitoring, response strategies)
  https://www.ibm.com/security
- Microsoft Incident Response Resources (threat monitoring, response, recovery)
  https://learn.microsoft.com/security

10. Work Based Learning and Professional Practice

- LinkedIn Learning Cybersecurity Skills (professional development, technical training)
  https://www.linkedin.com/learning
- Coursera Cybersecurity Programs (hands on skills, applied cybersecurity)
  https://www.coursera.org
- Google Cybersecurity Certificate (technical skills, workplace readiness)
  https://grow.google/certificates
- Harvard Online Cybersecurity Courses (professional practice, cybersecurity basics)
  https://online.hbs.edu

11. Leadership and Collaborative Security Operations

- MindTools Leadership Skills (leadership, teamwork, communication)
  https://www.mindtools.com
- Harvard Business Review Leadership (decision making, teamwork, leadership)
  https://hbr.org
- Atlassian Team Playbook (collaboration, project coordination, teamwork)
  https://www.atlassian.com/team-playbook
- Toastmasters Communication Skills (public speaking, leadership communication)
  https://www.toastmasters.org

12. Final Assessment Project

- GitHub (project documentation, collaboration, version control)
  https://github.com
- TryHackMe Cybersecurity Labs (hands on labs, security challenges, applications)
  https://tryhackme.com
- Cyber Range Exercises (simulation, security scenarios, testing)
  https://www.cyberbit.com
- Microsoft Learn Security Labs (hands on projects, cybersecurity skills)
  https://learn.microsoft.com/training

Technology Student Association – National Competitive Events

Software Development

Objective: *Students will design, implement, test, document, and present a software project with educational or social value aligned with TSA Software Development competition requirements.*

- Analyze the annual TSA Software Development theme and identify a societal need that can be addressed through software.
- Design a software tool, dashboard, interface, model, or application that responds to the selected need.
- Develop a functioning software solution using an appropriate programming language, platform, or development environment.
- Test and refine the project to improve functionality, usability, reliability, and accuracy.
- Document the software's purpose, design process, features, code structure, testing, and revisions.
- Submit the required code, URL, or PDF by the TSA deadline.
- Present the project's functionality, design process, and value, then respond to judge questions about the code.

Resources

- Technology Student Association – Software Development competition guidelines https://tsaweb.org/competitions-programs/tsa/themes-problems
- Cybersecurity & Infrastructure Security Agency – Cybersecurity resources https://www.cisa.gov/cybersecurity
- OWASP – Web application security resources https://owasp.org/
- GitHub Docs – Version control and project collaboration https://docs.github.com/

Technology Student Association – National Competitive Events

Data Science and Analytics

Objective: *Students will collect, analyze, visualize, document, and present a data set connected to the annual TSA Data Science and Analytics theme.*

- Research the annual TSA Data Science and Analytics theme and identify a focused topic for investigation.
- Collect or compile a data set of at least 500 rows from credible and relevant sources.
- Analyze data to identify trends, patterns, relationships, limitations, and possible predictions.
- Create a digital scientific poster that communicates the research question, data source, visualizations, analysis, and findings.
- Prepare a documentation portfolio explaining methods, data collection, analysis, conclusions, and resources.
- Present the digital scientific poster within the TSA time limit using clear, evidence-based communication.
- Complete an on-site semifinal challenge by creating a visual representation and brief synopsis from a provided data set.

Resources

- Technology Student Association – Data Science and Analytics competition guidelines
  https://tsaweb.org/competitions-programs/tsa/themes-problems
- Kaggle Datasets – Public data sets for analysis
  https://www.kaggle.com/datasets
- Google Dataset Search
  https://datasetsearch.research.google.com/
- Tableau Public – Data visualization tools
  https://public.tableau.com/

Technology Student Association – National Competitive Events

Debating Technological Issues

Objective: *Students will research, document, organize, and defend evidence-based arguments about technological issues in alignment with TSA Debating Technological Issues competition requirements.*

- Research the annual TSA debate topic and related subtopics from credible sources.
- Prepare a one-page summary of references using MLA format according to TSA competition requirements.
- Develop evidence-based pro and con arguments for multiple technological issue subtopics.
- Organize claims, evidence, reasoning, cross-examination questions, and rebuttal points for timed debate rounds.
- Use clear, concise, and persuasive language appropriate for a formal debate setting.
- Respond to opposing arguments through questioning, analysis, and rebuttal.
- Evaluate debate performance using TSA criteria for research, argument quality, communication, reasoning, and professionalism.

Resources

- Technology Student Association – Debating Technological Issues competition guidelines
  https://tsaweb.org/competitions-programs/tsa/themes-problems
- Purdue OWL – MLA Formatting and Style Guide
  https://owl.purdue.edu/owl/researchandcitation/mlastyle/mlaformattingandstyleguide/
- National Speech & Debate Association – Debate resources
  https://www.speechanddebate.org/
- Cybersecurity & Infrastructure Security Agency – Cybersecurity guidance and current issues
  https://www.cisa.gov/cybersecurity