COLORADO STATE UNIVERSITY GLOBAL

# ISM529: EMERGING CYBERSECURITY TECHNOLOGY, THREATS, AND DEFENSES

**Credit Hours**: 3

**Contact Hours:** This is a 3-credit course, offered in accelerated format. This means that 16 weeks of material is covered in 8 weeks. The exact number of hours per week that you can expect to spend on each course will vary based upon the weekly coursework, as well as your study style and preferences. You should plan to spend 14-20 hours per week in each course reading material, interacting on the discussion boards, writing papers, completing projects, and doing research.

**Faculty Information:** Faculty contact information and office hours can be found on the faculty profile page.

## COURSE DESCRIPTION AND OUTCOMES

### Course Description:

This course provides students with the ability to explore and examine emerging trends and technology in cybersecurity. Students will analyze organizations and review the feasibility of adopting new cybersecurity trends to provide competitive advantages in the workplace. This course also evaluates how policies and procedures continue to evolve as technology changes and becomes more capable in the workplace.

### Course Overview:

In this course, you will learn about the basic elements regarding cybersecurity. Topics will include types of cyberattacks, defense against cyberattacks, encryption, VPNs, OS hardening, and cyber policy and standards development. You will engage with each other in discussion around these important cybersecurity topics and will ultimately design your own cybersecurity policy. Each week contains not only textbook readings but also required and recommended article readings that convey current and relevant information in the field of cybersecurity. Each module also contains videos to help supplement your learning.

### Course Learning Outcomes:

1. Evaluate the roles of security and privacy with respect to the information and communication of an organization.
2. Appraise the concepts of security and privacy and how the imperatives for each may compliment or interfere with the imperative for the other.
3. Evaluate how the basic threats, vulnerabilities, risks, and attacks on IT networks have evolved over time.
4. Analyze the implications of major emerging technology trends, issues, and threats to the security and privacy of networks and information.
5. Design policy and practices to defend against emerging security and privacy threats.

## PARTICIPATION & ATTENDANCE

Prompt and consistent attendance in your online courses is essential for your success at CSU-Global Campus. Failure to verify your attendance within the first seven days of this course may result in your withdrawal. If for some reason you would like to drop a course, please contact your advisor.

Online classes have deadlines, assignments, and participation requirements just like on-campus classes. Budget your time carefully and keep an open line of communication with your instructor. If you are having technical problems, problems with your assignments, or other problems that are impeding your progress, let your instructor know as soon as possible.

## COURSE MATERIALS

**Required:**

Easttom, C. (2018). *Network defense and countermeasures: Principles and practices* (3rd ed.). New York, NY: Pearson.

- Print ISBN: 9780789759962
- eText ISBN: 9780134893099

***NOTE:*** *All non-textbook required readings and materials necessary to complete assignments, discussions, and/or supplemental or required exercises are provided within the course itself. Please read through each course module carefully.*

## COURSE SCHEDULE

### Due Dates

The Academic Week at CSU-Global begins on Monday and ends the following Sunday.

- **Discussion Boards:** The original post must be completed by Thursday at 11:59 p.m. MT and Peer Responses posted by Sunday 11:59 p.m. MT. Late posts may not be awarded points.
- **Critical Thinking:** Assignments are due Sunday at 11:59 p.m. MT.

## WEEKLY READING AND ASSIGNMENT DETAILS

### Module 1

**Readings**

- Chapters 1 & 2 in *Network Defense and Countermeasures: Principles and Practices*
- Lopez, O. (2016). A hacker and a refugee walk into a bar. *Newsweek Global, 167*(3), 46.
- Chapman, S., Smith, R., Maglaras, L., & Janicke, H. (2017). Can a network attack be simulated in an emulated environment for network security training*? Journal of Sensor and Actuator Networks, 6*(3), 16. Retrieved from https://www.mdpi.com/2224-2708/6/3/16/htm

**Discussion (25 points)**

**Critical Thinking (75 points)**

**Option #1: Recent Security Breaches**

The firm that you work for is concerned about the malware attacks that have been occurring around the world. You have been asked by the head of the IT department to research two security breaches that have occurred in the last two years. One should be from the United States and the other from another country. Describe the details of each attack. Then, discuss how each could have been prevented and contained with applicable examples and details from this week's readings.

Your paper should be 3-5 pages in length (excluding cover page and references page) and conform to CSU-Global Guide to Writing and APA. Include at least two scholarly references in addition to the course textbook, for a total of three sources minimum. The CSU-Global Library is a good place to find these references.

**Option #2 CIA Triad and Data Integrity Violations**

The goals of information security--Confidentiality, Integrity, and Availability--are referred to as the CIA Triad. In this week's critical thinking activity, discuss the concept of the CIA triad, while providing relevant examples of each of the three goals. Additionally, give three examples of data integrity violations. Please provide detailed information on all three examples within your paper.

Your paper should be 3-5 pages in length (excluding cover page and references page) and conform to CSU-Global Guide to Writing and APA. Include at least two scholarly references in addition to the course textbook, for a total of three sources minimum. The CSU-Global Library is a good place to find these references.

## Module 2

**Readings**

- Chapters 6 & 7in *Network Defense and Countermeasures: Principles and Practices*
- Kamp, P. (2016). More encryption means less privacy. *Communications of the ACM, 59*(4), 40-42.
- Aswad, S., & Qasim, M. (2017). A solution to enhance VPN effect on wireless network performance. *Nahrain University, College of Engineering Journal, 16*(1), 102-110.

**Discussion (25 points)**

**Critical Thinking (75 points)**

**Option #1: Historical Encryption**

For your critical thinking assignment this week, research an encryption method that has been used historically but is no longer used (such as the Enigma cipher of the Germans in World War II). Describe how that encryption method works, paying particular attention to how it contrasts with more modern methods. Be sure to discuss at least one modern method in your comparison.

Your paper should be 4-6 pages in length (excluding title and reference pages) and conform to CSU-Global Guide to Writing and APA. Include at least two scholarly references in addition to the course textbook. The CSU-Global Library is a good place to find these references.

**Option #2: Comparing Authentication Protocols**

For your critical thinking assignment this week, research VPN authentication protocols. Compare the protocols by pointing out the strengths and weaknesses of each. Which one would you recommend for your company? Provide appropriate justifications for your decision.

Your paper should be 4-6 pages in length (excluding title and reference pages) and conform to CSU-Global Guide to Writing and APA. Include at least two scholarly references in addition to the course textbook.  The CSU-Global Library is a good place to find these references.

## Module 3

**Readings**

- Chapters 5 & 8 in *Network Defense and Countermeasures: Principles and Practices*
- Ahmed, H. M., Hassan, N. F., & Fahad, A. A. (2017). Designing a smartphone honeypot system using performance counters. *Journal of Modern Science, 3*(1), 46-52. Retrieved from https://www.sciencedirect.com/science/article/pii/S2405609X16304225
- Waheed, F., & Ali, M. (2018). Hardening CISCO devices based on cryptography and security protocols - part one: background theory. *Annals of Emerging Technologies in Computing, 2*(3), 27-44. Retrieved from https://doaj.org/article/71e3c8aac24546e3abb01418da72f626

**Discussion (25 points)**

**Critical Thinking (75 points)**

**Option #1: Improving Honeypots**

By now you should have a good understanding of how honeypots work. Like all security technology, honeypots are evolving. As you start your paper, discuss a brief background of honeypots including how they have evolved over the years. Then, describe in detail at least three improvements you would recommend in honeypot technology. This could include features not currently available, improved detection, or more aggressive responses.

Here are some sites that may be useful as you prepare your assignment this week:

- Project Honey Pot
- Honeypots: The Sweet Spot in Network Security

References:

- (2019). Project Honey Pot. Retrieved from https://www.projecthoneypot.org/
- Harrison, J. (2003). Honeypots: The sweet spot in network security. Retrieved from https://www.computerworld.com/article/2573345/honeypots--the-sweet-spot-in-network-security.html

Your paper should be 4-6 pages in length (excluding title and reference pages) and conform to CSU-Global Guide to Writing and APA. Include at least two scholarly references in addition to the course textbook. The CSU-Global Library is a good place to find these references.

**Option #2: OS Hardening Analysis**

Starting with a discussion on operating system hardening, evaluate the advantages and disadvantages to OS hardening. Although many of the same security concepts that apply to Windows also apply to Linux, explain the differences in configuration. Lastly, discuss whether or not to include data protection in OS hardening efforts.

Your paper should be 4-6 pages in length (excluding title and reference pages) and conform to CSU-Global Guide to Writing and APA. Include at least two scholarly references in addition to the course textbook. The CSU-Global Library is a good place to find these references.

**Portfolio Milestone (50 points)**

**Option #1: Computer and Internet Security Policy**

You have been hired as the CSO (Chief Security Officer) for an organization. Your job is to develop a computer and internet security policy for the organization that covers four key areas as your final project due in Module 8 (as explained in the Portfolio Project Option #1 overview). In this first milestone, you will submit the first area--Computer and Email Acceptable Use Policy. Please draft this policy portion of your final project.

The Computer and Email Acceptable Use Policy portion of your Portfolio Project should be 3-5 pages in length (excluding title and reference pages) and conform to CSU-Global Guide to Writing and APA. Include at least two scholarly references in addition to the course textbook. The CSU-Global Library is a good place to find these references.

**Option #2: Disaster Recovery Plan**

You will develop a disaster recovery plan for an organization as your final project due in Module 8. Your plan will cover eight sections (as explained in the Portfolio Project Option #2 overview). In this first milestone, you will write the first three sections for the final project:

1. Important: This section should summarize key action steps (such as where to assemble employees if forced to evacuate the building) and list key contacts with contact information for ease of authorizing and launching the plan.
2. Introduction
3. Roles and Responsibilities

The first three sections of your Portfolio Project should be 3-5 pages in length (excluding title and reference pages) and conform to CSU-Global Guide to Writing and APA. Include at least two scholarly references in addition to the course textbook. The CSU-Global Library is a good place to find these references.

## Module 4

**Readings**

- Chapters 9 & 10 in *Network Defense and Countermeasures: Principles and Practices*
- Heller, M. (2018). Atlanta hack highlights ransomware dangers. *CFO: The Magazine for Senior Financial Executives, 34*(3), 6. Retrieved from https://www.cfo.com/cyber-security-technology/2018/03/atlanta-hack-highlights-ransomeware-dangers/

**Discussion (25 points)**

**Critical Thinking (75 points)**

**Option #1: Effects of Viruses on Computer Performance**

For this activity, write a research paper answering the following questions as if you are preparing a report for management within your organization.

- What are the effects of viruses on the company's computer systems?
- What are the control measures the company can use to secure computer systems against viruses?
- What are some software tools that the company can implement to improve computer performance?
- What are some policy measures the company should implement regarding preventing virus attacks on their computer systems?

Your paper should be 4-6 pages in length (excluding title and reference pages) and conform to CSU-Global Guide to Writing and APA. Include at least two scholarly references in addition to the course textbook.  The CSU-Global Library is a good place to find these references.

**Option #2: Anti-Spyware Policy**

Create an anti-spyware policy for your organization or for CSU-Global. Please review a sample template (Malicious Code, Spam, and Spyware Protection Policy Sample) to assist with creating your policy.

Reference:

(n.d.). Malicious code, spam and spyware protection policy sample. Retrieved from https://www.michigan.gov/documents/msp/Sample_Malicious_Code_Spam_Spyware_Protection_Policy_441713_7.pdf

Your paper should be 4-6 pages in length (excluding title and reference pages) and conform to CSU-Global Guide to Writing and APA. Include at least two scholarly references in addition to the course textbook. The CSU-Global Library is a good place to find these references.

## Module 5

**Readings**

- Chapters 11 & 13 in *Network Defense and Countermeasures: Principles and Practices*
- Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security, 61*, 169-183.

- Vincent, N. E. (2016). A holistic approach to IT risk: The COBIT framework can help auditors understand and address their organization's technology risks. *Internal Auditor, 73*(6), 18.

## Discussion (25 points)

## Critical Thinking (75 points)

### Option #1: Academic User Policies

Create a document that defines end user policies in an academic setting. These policies should clearly define acceptable and unacceptable use for all personnel. There can be separate policies for administration, faculty, and students.

Your paper should be 4-6 pages in length (excluding title and reference pages) and conform to CSU-Global Guide to Writing and APA. Include at least two scholarly references in addition to the course textbook. The CSU-Global Library is a good place to find these references.

### Option #2: Risk Assessment Using NIST

Using NIST SP 800-30 (discussed in Chapter 13), discuss how you would perform a risk assessment for a small network. Be sure to provide an overview of NIST SP 800-30 prior to conducting the risk assessment.

Your paper should be 4-6 pages in length (excluding title and reference pages) and conform to CSU-Global Guide to Writing and APA. Include at least two scholarly references in addition to the course textbook. The CSU-Global Library is a good place to find these references.

## Portfolio Milestone (50 points)

### Option #1: Computer and Internet Security Policy

You have been hired as the CSO (Chief Security Officer) for an organization. Your job is to develop a computer and internet security policy for the organization that covers four key areas as your final project due in Module 8 (as explained in the Portfolio Project Option #1 overview). In this second milestone, you will submit the second area--Internet Acceptable Use Policy. Please draft this policy portion of your final project.

The Internet Acceptable Use Policy portion of your Portfolio Project should be 3-5 pages in length (excluding title and reference pages) and conform to CSU-Global Guide to Writing and APA. Include at least two scholarly references in addition to the course textbook. The CSU-Global Library is a good place to find these references.

### Option #2: Disaster Recovery Plan

You will develop a disaster recovery plan for an organization as your final project due in Module 8. Your plan will cover eight sections (as explained in the Portfolio Project Option #2 overview). In this second milestone, you will write sections four and five:

- Incident Response
- Plan Activation

Sections four and five of your Portfolio Project should be 3-5 pages in length (excluding title and reference pages) and conform to CSU-Global Guide to Writing and APA. Include at least two scholarly references in addition to the course textbook. The CSU-Global Library is a good place to find these references.

## Module 6

**Readings**

- Chapter 12 in *Network Defense and Countermeasures: Principles and Practices*
- Antunes, N., & Vieira, M. (2017). Designing vulnerability testing tools for web services: Approach, components, and tools. *International Journal of Information Security, 16*(4), 435-457.
- Munodawafa, F., & Awad, A. I. (2018). Security risk assessment within hybrid data centers: A case study of delay sensitive applications. *Journal of Information Security and Applications, 43*, 61–72.

**Discussion (25 points)**

**Critical Thinking (75 points)**

### Option #1: Assessing Security Policies

Find a security policy online (or use one from your own organization). Summarize the organization's policies. Make recommendations for changes to enhance the organization's overall security posture. Draw comparisons from other resources, such as the course textbook, scholarly references, or other organizational security policies. How does your chosen organization's security policy compare to others? Additionally, please justify your recommendations.

Your paper should be 4-6 pages in length (excluding title and reference pages) and conform to CSU-Global Guide to Writing and APA. Include at least two scholarly references in addition to the course textbook. The CSU-Global Library is a good place to find these references.

### Option #2: Conducting the Initial Assessment

Assessing a system's security can be separated into the "six Ps": patch, ports, protect, policies, probe, and physical. Discuss why all six of these concepts are important to assessing a system's security and what role they plan in maintaining and supporting information security within an organization.

Your paper should be 4-6 pages in length (excluding title and reference pages) and conform to CSU-Global Guide to Writing and APA. Include at least two scholarly references in addition to the course textbook. The CSU-Global Library is a good place to find these references.

### Portfolio Reminder

A final Portfolio Project is due at the end of the course. You have **two options** from which to choose for this final project. This week, you should continue to work on the Portfolio Project and review the Portfolio Project grading rubric.

## Module 7

**Readings**

- Chapters 14 & 15 in *Network Defense and Countermeasures: Principles and Practices*
- Cervone, H. (2017). Disaster recovery planning and business continuity for informaticians. *Digital Library Perspectives, 33*(2), 78-81.

**Discussion (25 points)**

**Portfolio Reminder**

A final Portfolio Project is due at the end of the course. You have **two options** from which to choose for this final project. This week, you should continue to work on the Portfolio Project and review the Portfolio Project grading rubric.

## Module 8

**Readings**

- Chapter 17 in *Network Defense and Countermeasures: Principles and Practices*
- Close-Up Media. (2018, November). Symantec reveals new cyber espionage group targeting government, military and defense sectors. *Professional Services Close – Up*.
- Warf, B., & Fekete, F. (2016). Relational geographies of cyberterrorism and cyberwar. *Space & Polity, 20*(2), 143-57.

**Discussion (25 points)**

**Portfolio Project (250 points)**

**Option #1: Computer and Internet Security Policy**

You have been hired as the CSO (Chief Security Officer) for an organization. Your job is to develop a computer and internet security policy for the organization that covers the following areas:

1. Computer and email acceptable use policy
2. Internet acceptable use policy
3. Password protection policy
4. Social media and blogging policy.

Make sure you are sufficiently specific in addressing each area. There are plenty of security policy and guideline templates available online for you to use as a reference or for guidance. Your plan should reflect the business model and corporate culture of the specific organization you selected. Be sure to consider all concepts presented in this course.

Your paper should be 10-15 pages in length and conform to CSU-Global Guide to Writing and APA. Include at least six scholarly references in addition to the course textbook. The CSU-Global Library is a good place to find these references.

**Option #2: Disaster Recovery Plan**

Develop a disaster recovery plan for an organization. There are many different templates available online for you to use as reference and guidance. Your plan should cover the following sections (these sections detail the elements in a DR plan in the sequence defined by industry compliance standards ISO 27031 and ISO 24762):

1. Important: This section should summarize key action steps (such as where to assemble employees if forced to evacuate the building) and list key contacts with contact information for ease of authorizing and launching the plan.
2. Introduction
3. Roles and Responsibilities
4. Incident Response
5. Plan Activation
6. Document History
7. Procedures
8. Appendices: Located at the end of the plan, these can include systems inventories, application inventories, network asset inventories, contracts and service-level agreements, supplier contact data, and any additional documentation that will facilitate recovery.

Your paper should be 10-15 pages in length and conform to CSU-Global Guide to Writing and APA. Include at least six scholarly references in addition to the course textbook. The CSU-Global Library is a good place to find these references.

## COURSE POLICIES

| Grading Scale | |
|---|---|
| A | 95.0 – 100 |
| A- | 90.0 – 94.9 |
| B+ | 86.7 – 89.9 |
| B | 83.3 – 86.6 |
| B- | 80.0 – 83.2 |
| C+ | 75.0 – 79.9 |
| C | 70.0 – 74.9 |
| D | 60.0 – 69.9 |
| F | 59.9 or below |

**Course Grading**

20% Discussion Participation
45% Critical Thinking Assignments
35% Final Portfolio Project

## IN-CLASSROOM POLICIES

For information on late work and incomplete grade policies, please refer to our **In-Classroom Student Policies and Guidelines** or the Academic Catalog for comprehensive documentation of CSU-Global institutional policies.

### Academic Integrity

Students must assume responsibility for maintaining honesty in all work submitted for credit and in any other work designated by the instructor of the course. Academic dishonesty includes cheating, fabrication, facilitating academic dishonesty, plagiarism, reusing /re-purposing your own work (see *CSU-Global Guide to Writing and APA* for percentage of repurposed work that can be used in an assignment), unauthorized possession of academic materials, and unauthorized collaboration. The CSU-Global Library provides information on how students can avoid plagiarism by understanding what it is and how to use the Library and Internet resources.

### Citing Sources with APA Style

All students are expected to follow the *CSU-Global Guide to Writing and APA* when citing in APA (based on the APA Style Manual, 6th edition) for all assignments. For details on CSU-Global APA style, please review the APA resources within the CSU-Global Library under the “APA Guide & Resources” link. A link to this document should also be provided within most assignment descriptions in your course.

### Disability Services Statement

CSU–Global is committed to providing reasonable accommodations for all persons with disabilities. Any student with a documented disability requesting academic accommodations should contact the Disability Resource Coordinator at 720-279-0650 and/or email ada@CSUGlobal.edu for additional information to coordinate reasonable accommodations for students with documented disabilities.

### Netiquette

Respect the diversity of opinions among the instructor and classmates and engage with them in a courteous, respectful, and professional manner. All posts and classroom communication must be conducted in accordance with the student code of conduct. Think before you push the Send button. Did you say just what you meant? How will the person on the other end read the words?

Maintain an environment free of harassment, stalking, threats, abuse, insults or humiliation toward the instructor and classmates. This includes, but is not limited to, demeaning written or oral comments of an ethnic, religious, age, disability, sexist (or sexual orientation), or racist nature; and the unwanted sexual advances or intimidations by email, or on discussion boards and other postings within or connected to the online classroom. If you have concerns about something that has been said, please let your instructor know.