



**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 an overview of cybersecurity threats, compromises and the related protection mechanisms. Topics include security of communications, networks and infrastructures. The course also discusses best practices in security policy formulation, cyber forensics and prevention of cybercrimes. Overall, the course introduces the latest developments in the field.

### **Course Overview:**

Concern for cybersecurity is real. Organizations today are more vulnerable to logical attacks than ever before. The reasons for such cyber-attacks are countless, and protection against them is tenuous at best. While motivation for the attacks might range from personal gain to theft of proprietary information to corporate fraud and terrorism, protection demands that adequate measures are put in place that ensure the security and integrity of an enterprise.

This course provides an overview of cybersecurity threats, compromises and the related protection mechanisms. Topics include security of communications, networks and infrastructures. The course also discusses best practices in security policy formulation, cyber forensics and prevention of cybercrimes. Overall, the course introduces the latest developments in the field.

### **Course Learning Outcomes:**

1. Develop the ability to recognize technical and organizational computer security issues within the global environment.
2. Understand global cyberstalking and cyberterrorism laws.
3. Understand current security vulnerabilities and their impact on business.
4. Understand the importance of computer forensics.
5. Develop an understanding of security policies and how they can help business.
6. Evaluate the impact of cyber-threats and corporate espionage activities on organizational security.
7. Define the benefits and problems with encryption.

---

## 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 7 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:

Textbook (required): Easttom, C. (2016). *Computer security fundamentals* (3rd ed.). Indianapolis, IN: Pearson. ISBN-13: 9780789757463

### Suggested:

Textbook (recommended): Singer, P. W. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford: Oxford University Press. ISBN-10: 0199918112

**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 at 11:59 p.m. MT. Late posts may not be awarded points.
- **Opening Exercises:** Take the Opening Exercise before reading each week's content to see which areas you will need to focus on. You may take these exercises as many times as you need. The Opening Exercises will not affect your final grade.
- **Mastery Exercises:** Students may access and retake Mastery Exercises through the last day of class until they achieve the scores they desire.
- **Critical Thinking:** Assignments are due Sunday at 11:59 p.m. MT.

---

## WEEKLY READING AND ASSIGNMENT DETAILS

---

### Module 1

#### Readings

· Chapters 1 & 2 in *Computer Security Fundamentals*

### Opening Exercise (0 points)

### Discussion (25 points)

### Critical Thinking (60 points)

Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

#### Option #1: WikiLeaks Case Study

Consider this WikiLeaks case study available in the CSU-Global Library on ProQuest:

Oliver, M.C. (2017). WikiLeaks under fire: Is it electronic civil disobedience? *Oxímora. Revista Internacional De Ética Y Política*, (10), 182-193.

The disclosures at WikiLeaks have raised significant concerns about the damage caused by leaks. Some claim that in many ways, the Wiki Leaks founder, Julian Assange, was terrorizing nation states and corporations. What corporate and/or national policy initiative do you think should be put in place to curb such forms of cyberterrorism?

Your paper should meet the following requirements:

- Be 2-3 pages in length, not including the cover page and reference page.
- Follow the CSU-Global Guide to Writing and APA. Each paper should include an introduction, a body with at least two fully developed paragraphs, and a conclusion.
- Support your answers with the readings from Module 1 and at least one scholarly journal article. The CSU-Global Library is a great place to find resources.
- Be clearly and well written, concise, and logical, using excellent grammar and style techniques. You are being graded in part on the quality of your writing. If you need assistance with your writing style, start with Tools for Effective Writing at the CSU-Global Library, accessible from the Library's homepage.

#### Option #2: Advanced Persistent Threats

Advanced Persistent Threats (APT) is a network under attack. The attack stays undetected for a long period of time. The intention is to not set off any alarms, to not cause damage, but to steal as much data as possible from an organization over time.

1. What can be done to protect an organization against this type of attack?
2. What can be done to detection an APT?
3. What tools can be used to identify and eradicate the treat?

Your paper should meet the following requirements:

- Be 2-3 pages in length, not including the cover page and reference page.
- Follow the CSU-Global Guide to Writing and APA. Each paper should include an introduction, a body with at least two fully developed paragraphs, and a conclusion.
- Support your answers with the readings from Module 1 and at least one scholarly journal article. The CSU-Global Library is a great place to find resources.
- Be clearly and well written, concise, and logical, using excellent grammar and style techniques. You are being graded in part on the quality of your writing. If you need assistance with your

writing style, start with Tools for Effective Writing at the CSU-Global Library, accessible from the Library's homepage.

### **Mastery Exercise (10 points)**

## **Module 2**

### **Readings**

- Chapter 3 in *Computer Security Fundamentals*

### **Opening Exercise (0 points)**

### **Discussion (25 points)**

### **Critical Thinking (60 points)**

Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

#### **Option #1: Cyberstalking Case Studies**

There are several convicted cases of cyberstalking and internet fraud/abuse (e.g., Misha Glenny, a UK-based journalist, recently wrote a book on the subject matter appropriately titled *Dark Markets*). For this critical thinking assignment, you are required to scan the popular press (especially *Wall Street Journal*) and find at least five cases of individuals who have been convicted of cyberstalking, fraud and abuse. Document each case and provide a brief synopsis. What issues do these cases bring to light? What laws might attach?

Warman, M. (2011, October). Dark market: Cyberthieves, cybercops and you by Misha Glenny: Review.

Your paper should meet the following requirements:

- Be approximately two pages in length, not including the cover page and reference page.
- Follow the CSU-Global Guide to Writing and APA. Each paper should include an introduction, a body with at least two fully developed paragraphs, and a conclusion.
- Support your answers with the readings from Module 2 and at least one scholarly journal article. The CSU-Global Library is a great place to find resources.
- Be clearly and well written, concise, and logical, using excellent grammar and style techniques. You are being graded in part on the quality of your writing. If you need assistance with your writing style, start with Tools for Effective Writing at the CSU-Global Library, accessible from the Library's homepage.

#### **Option #2: Identify Theft Case Studies**

Identity theft is a big problem. In 2014 there was a victim of identity theft every two seconds according to a study released by Javelin Strategy & Research (see reference below). This research also found that \$16 billion was stolen from 12.7 million U.S. consumers in 2014, compared with \$18 billion and 13.1 million victims a year earlier. Find at least five cases of identity theft. Describe ways you can protect yourself from identity theft. What laws might attach?

\$16 billion stolen from 12.7 million identity fraud victims in 2014, according to Javelin Strategy & Research. (2015, March). *Javelin Strategy*. Retrieved from <https://www.javelinstrategy.com/press-release/16-billion-stolen-127-million-identity-fraud-victims-2014-according-javelin-strategy>

Your paper should meet the following requirements:

- Be approximately two pages in length, not including the cover page and reference page.
- Follow the CSU-Global Guide to Writing and APA. Each paper should include an introduction, a body with at least two fully developed paragraphs, and a conclusion.

- Support your answers with the readings from Module 2 and at least one scholarly journal article. The CSU-Global Library is a great place to find resources.
- Be clearly and well written, concise, and logical, using excellent grammar and style techniques. You are being graded in part on the quality of your writing. If you need assistance with your writing style, start with Tools for Effective Writing at the CSU-Global Library, accessible from the Library's homepage.

### **Mastery Exercise (10 points)**

## **Module 3**

### **Readings**

- Chapters 4, 5 & 6 in *Computer Security Fundamentals*
- Melendez, M. (2015). *Ransomware: An analysis of a growing threat landscape* (Capstone Project). Retrieved from ProQuest Dissertations & Theses Global. (1752223374).

### **Opening Exercise (0 points)**

### **Discussion (25 points)**

### **Critical Thinking (60 points)**

Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

#### **Option #1: Cyber Attacks**

In a well-written paper, write a response to three of the following five questions:

1. What are the common tools used to protect against a DoS (Denial of Service) or DDoS (Distributed Denial-of-Service) attack?
2. What is malware and how does it spread?
3. What is a Buffer-Overflow attack?
4. How does a SQL injection attack take place?
5. What are some of the tools that a hacker can use to crack passwords?

Your paper should meet the following requirements:

- Be 2-3 pages in length, not including the cover page and reference page.
- Follow the CSU-Global Guide to Writing and APA. Each paper should include an introduction, a body with at least two fully developed paragraphs, and a conclusion.
- Support your answers with the readings from Module 3 and at least one scholarly journal article. The CSU-Global Library is a great place to find resources.
- Be clearly and well written, concise, and logical, using excellent grammar and style techniques. You are being graded in part on the quality of your writing. If you need assistance with your writing style, start with Tools for Effective Writing at the CSU-Global Library, accessible from the Library's homepage.

#### **Option #2: Ransomware**

Ransomware is expected to grow according to the FBI (Devlin, 2016). According to this same article there were 2,453 reported incidents of ransomware in 2015. In one case it cost a hospital in California paid out \$17,000 dollars in ransom to restore the data locket by hackers. This type of malware encrypts critical computer information and locks it until ransom is paid. This technique of encryption is called

“Cryptolocker.” Find at least five cases of ransomware. Describe ways an organization can protect itself from ransomware. What laws might apply?

Your paper should meet the following requirements:

- Be 2-3 pages in length, not including the cover page and reference page.
- Follow the CSU-Global Guide to Writing and APA. Each paper should include an introduction, a body with at least two fully developed paragraphs, and a conclusion.
- Support your answers with the readings from Module 3 and at least one scholarly journal article. The CSU-Global Library is a great place to find resources.
- Be clearly and well written, concise, and logical, using excellent grammar and style techniques. You are being graded in part on the quality of your writing. If you need assistance with your writing style, start with Tools for Effective Writing at the CSU-Global Library, accessible from the Library’s homepage.

#### **Mastery Exercise (10 points)**

#### **Portfolio Milestone (10 points)**

Review the instructions for the Portfolio Project in Module 8. Submit your portfolio topic in the assignment drop box. Include a paragraph describing why you chose that topic and what problems you may anticipate in researching your subject.

### **Module 4**

#### **Readings**

- Chapter 7 in *Computer Security Fundamentals*

#### **Opening Exercise (0 points)**

#### **Discussion (25 points)**

#### **Critical Thinking (60 points)**

Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

#### **Option #1: Cyber espionage**

Cyber espionage is term used to illicit access to confidential information. Spying or deploying malware to steal or destroy data within a computer network. This can apply to a government agencies or enterprise.

1. Describe corporate espionage
2. Define at least three ways to prevent it

Your paper should meet the following requirements:

- Be 2-3 pages in length, not including the cover page and reference page.
- Follow the CSU-Global Guide to Writing and APA. Each paper should include an introduction, a body with at least two fully developed paragraphs, and a conclusion.
- Support your answers with the readings from Module 4 and at least one scholarly journal article. The CSU-Global Library is a great place to find resources.
- Be clearly and well written, concise, and logical, using excellent grammar and style techniques. You are being graded in part on the quality of your writing. If you need assistance with your writing style, start with Tools for Effective Writing at the CSU-Global Library, accessible from the Library’s homepage.

#### **Option #2: Cyber Terrorism**

In a well-written paper, write a response to one of the following questions:

1. Is cyber terrorism a serious threat? Is the United States making adequate preparations against cyberterrorism?
2. In recent years, several cyber-attacks supported by national governments are believed to have taken place. Have these attacks generally achieved their goals? Were the governments wise to launch the attacks?

Your paper should meet the following requirements:

- Be 2-3 pages in length, not including the cover page and reference page.
- Follow the CSU-Global Guide to Writing and APA. Each paper should include an introduction, a body with at least two fully developed paragraphs, and a conclusion.
- Support your answers with the readings from Module 4 and at least one scholarly journal article. The CSU-Global Library is a great place to find resources.
- Be clearly and well written, concise, and logical, using excellent grammar and style techniques. You are being graded in part on the quality of your writing. If you need assistance with your writing style, start with Tools for Effective Writing at the CSU-Global Library, accessible from the Library's homepage.

**Mastery Exercise (10 points)**

## **Module 5**

### **Readings**

- Chapters 8 & 9 in *Computer Security Fundamentals*

**Opening Exercise (0 points)**

**Discussion (25 points)**

**Critical Thinking (60 points)**

Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

### **Option #1: Security and Encryption Policies**

Read the following case study available through ProQuest (CSU-Global Library):

Chinese National pleads guilty to conspiring to hack into US Defense Contractors' systems to steal sensitive military information. (2016, March). *US Fed News Service, Including US State News*.

Answer the following questions in your paper:

1. What strategic recommendations would you make?
2. What operational security aspects should be considered to prevent such attacks in the future?
3. What sort of an encryption policy, if any, would have helped in this situation?

Your paper should meet the following requirements:

- Be 1-2 pages in length, not including the cover page and reference page.
- Follow the CSU-Global Guide to Writing and APA. Each paper should include an introduction, a body with at least two fully developed paragraphs, and a conclusion.
- Support your answers with the readings from Module 5 and at least one scholarly journal article. The CSU-Global Library is a great place to find resources.

- Be clearly and well-written, concise, and logical, using excellent grammar and style techniques. You are being graded in part on the quality of your writing. If you need assistance with your writing style, start with Tools for Effective Writing at the CSU-Global Library, accessible from the Library's homepage.

### **Option #2: Cyber Attack Case Study**

Read the following case study available through ProQuest (CSU-Global Library):

Benyon, D. (2016, February). Cyber gets physical. *Reactions*.

Answer the following questions in your paper:

1. Describe at least two other physical cyber-attacks.
2. Could this type of attack affect our power grid, water supply, airline industry, nuclear plants, oil refineries and more?
3. What preventative measures can be used?

Your paper should meet the following requirements:

- Be 1-2 pages in length, not including the cover page and reference page.
- Follow the CSU-Global Guide to Writing and APA. Each paper should include an introduction, a body with at least two fully developed paragraphs, and a conclusion.
- Support your answers with the readings from Module 5 and at least one scholarly journal article. The CSU-Global Library is a great place to find resources.
- Be clearly and well written, concise, and logical, using excellent grammar and style techniques. You are being graded in part on the quality of your writing. If you need assistance with your writing style, start with Tools for Effective Writing at the CSU-Global Library, accessible from the Library's homepage.

### **Mastery Exercise (10 points)**

### **Portfolio Milestone (40 points)**

Submit an outline of your portfolio. Review the requirements of the portfolio in Module 8. The outline should reflect the topic you chose in Module 3 and cover all the required elements of the assignment. Include with your outline a draft of your proposed sources. Follow the CSU-Global Guide to Writing and APA.

## **Module 6**

### **Readings**

- Chapters 10 & 11 in *Computer Security Fundamentals*

### **Opening Exercise (0 points)**

### **Discussion (25 points)**

### **Critical Thinking (70 points)**

Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

### **Option #1: Insider Threats**

According to statistics insider threats pose the most potential for damage to data and network infrastructure. Do you agree? Or would you say the threat is external? What policies and procedures would you put into place to protect against these threats?

Your paper should meet the following requirements:

- Be 3-4 pages in length, not including the cover page and reference page.
- Follow the CSU-Global Guide to Writing and APA. Each paper should include an introduction, a body with at least two fully developed paragraphs, and a conclusion.
- Support your answers with the readings from Module 6 and at least one scholarly journal article. The CSU-Global Library is a great place to find resources.
- Be clearly and well written, concise, and logical, using excellent grammar and style techniques. You are being graded in part on the quality of your writing. If you need assistance with your writing style, start with Tools for Effective Writing at the CSU-Global Library, accessible from the Library's homepage.

### **Option #2: Cybersecurity Policy**

Write an essay on the topic "building and implementing a successful cybersecurity policy." The following content areas should be covered in the essay:

1. What would be a successful cybersecurity policy?
2. What are the ingredients of a typical cybersecurity policy?
3. How should the various elements of a cybersecurity policy be articulated?
4. What considerations should there be to implement the policy successfully?
5. How can you assure the ongoing success of the policy?

Your paper should meet the following requirements:

- Be 3-4 pages in length, not including the cover page and reference page.
- Follow the CSU-Global Guide to Writing and APA. Each paper should include an introduction, a body with at least two fully developed paragraphs, and a conclusion.
- Support your answers with the readings from Module 6 and at least one scholarly journal article. The CSU-Global Library is a great place to find resources.
- Be clearly and well written, concise, and logical, using excellent grammar and style techniques. You are being graded in part on the quality of your writing. If you need assistance with your writing style, start with Tools for Effective Writing at the CSU-Global Library, accessible from the Library's homepage.

### **Mastery Exercise (10 points)**

## **Module 7**

### **Readings**

- Chapter 12 in *Computer Security Fundamentals*

### **Opening Exercise (0 points)**

### **Discussion (25 points)**

### **Mastery Exercise (10 points)**

## **Module 8**

## Readings

- Chapters 13 & 14 in *Computer Security Fundamentals*

### Opening Exercise (0 points)

### Discussion (25 points)

### Mastery Exercise (10 points)

### Portfolio Project (300 points)

#### Option #1: Cybersecurity Case Studies

Throughout this course you have been collecting incidents of security breaches and potential mitigation strategies. For your final Portfolio assignment:

1. Submit a list of five cybersecurity breach case studies.
2. For each breach write a brief statement for each of the following points:
  - a. what went wrong
  - b. how could it have been prevented
  - c. what organizational measures should be instituted
3. Include examples of each breach, with dates of when the incident took place. Describe also the outcome.
4. In addition to your security breach case studies, write a short summary (two pages, 1.5 spacing) of your key learning points in management of cybersecurity within enterprises.

Submit your portfolio as a single document.

Your paper should meet the following requirements:

- Be approximately 10 pages in length, not including the cover page and reference page.
- Follow the CSU-Global Guide to Writing and APA. Each paper should include an introduction, a body with at least two fully developed paragraphs, and a conclusion.
- Support your answers with the readings from the course and at least four scholarly journal articles. The CSU-Global Library is a great place to find resources.
- Be clearly and well written, concise, and logical, using excellent grammar and style techniques. You are being graded in part on the quality of your writing. If you need assistance with your writing style, start with Tools for Effective Writing at the CSU-Global Library, accessible from the Library's homepage.

In Week 3, you will submit your topic choice and in Week 5, you will submit an outline of your project.

#### Option #2: Security Breach Case Studies

Throughout this course you have been learning about real-world security breaches and potential mitigation strategies. For your final Portfolio assignment answer the following questions:

- What cyber threat concerns you the most?
- What are the emerging and future technologies that we will have to worry the most about from a security perspective?
- What is the role of government in securing cyberspace?
- Where does the responsibility of private firms begin and end in cybersecurity?
- What can be done from a global perspective?

Submit your portfolio as a single document.

Your paper should meet the following requirements:

- Be approximately 10 pages in length, not including the cover page and reference page.
- Follow the CSU-Global Guide to Writing and APA. Each paper should include an introduction, a body with at least two fully developed paragraphs, and a conclusion.
- Support your answers with the readings from the course and at least four scholarly journal articles. The CSU-Global Library is a great place to find resources.
- Be clearly and well written, concise, and logical, using excellent grammar and style techniques. You are being graded in part on the quality of your writing. If you need assistance with your writing style, start with Tools for Effective Writing at the CSU-Global Library, accessible from the Library's homepage.

In Week 3, you will submit your topic choice and in Week 5, you will submit an outline of your project.

---

## 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  
0% Opening Exercises  
8% Mastery Exercises  
37% 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 /repurposing your own work (see CSU-Global Guide to Writing & 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 & APA when citing in APA (based on the most recent APA style manual) for all assignments. A link to this guide 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](mailto: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.