ITS360: Introduction to Cyber Security and Digital Crime

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.

Course Description and Outcomes

Course Description:
This course provides you with an introduction to cyber security and digital crime. You will learn about information security threats, dangers, and risks that organizations face in the workplace. You’ll also gain the ability to analyze potential vulnerabilities that can have an adverse impact on digital assets.

Course Overview:
Welcome to Introduction to Cyber Security and Digital Crime! This course provides students of information technology an introduction to cyber security and digital crime. You will learn about information security threats, dangers, and risks that organizations face in the workplace. This course will teach you to analyze vulnerabilities to digital crime that can jeopardize the security of businesses’ digital assets.

Course Learning Outcomes:

1. Demonstrate the ability to differentiate between various types of systems security threats that can lead to the loss of a major system security goal.
2. Analyze potential enterprise security vulnerabilities at various business sectors.
3. Demonstrate understanding of security vulnerabilities and loss effects and consequences that can have adverse impact on digital assets.
4. Analyze enterprise security needs and provide recommendations to best suit enterprise technology infrastructure.
5. Apply various security models and measures to enterprise infrastructure.
6. Demonstrate comparative understanding of benefits gained from applying various security measures to enterprise infrastructure.
7. Define and discuss types of computer crime, intellectual property, and codes of ethics in Information technology professions.

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

Textbook Information is located in the CSU-Global Booklist on the Student Portal.

### 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 12 midnight MT and Peer Responses posted by Sunday 12 midnight 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 Activities**: Assignments are due Sunday at 12 midnight MT.

<table>
<thead>
<tr>
<th>Week #</th>
<th>Readings</th>
<th>Assignments</th>
</tr>
</thead>
</table>
| 1      | • Chapter 1 in *Computer Security: Principles and Practice*  
• Mastery (10 points)  
• Critical Thinking (75 points) |
| 2      | • Chapter 3 in *Computer Security: Principles and Practice*  
• Mastery (10 points)  
• Critical Thinking (75 points)  
• Portfolio Project Milestone (25 points) |
| 3 | Chapter 6 in *Computer Security: Principles and Practice*  
Mastery (10 points)  
Critical Thinking (75 points) |
| 4 | Chapter 14 in *Computer Security: Principles and Practice*  
Mastery (10 points) |
| 5 | Chapter 15 in *Computer Security: Principles and Practice*  
Mastery (10 points)  
Critical Thinking (70 points) |
| 6 | Chapter 16 in *Computer Security: Principles and Practice*  
Mastery (10 points)  
Critical Thinking (75 points)  
Portfolio Project Milestone (25 points) |
| 7 | Chapter 17 in *Computer Security: Principles and Practice*  
Mastery (10 points) |
| 8 | Chapter 19 in *Computer Security: Principles and Practice*  
Mastery (10 points)  
Portfolio (300 points) |
Assignment Details

This course includes the following assignments/projects:

Module 1

Critical Thinking Assignment (75 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 Vulnerabilities and Loss of Attainable Goals
You have been hired by a small company of 50 employees to manage its IT department. The company’s CEO meets with you and asks you to prepare a report pointing out potential security vulnerabilities at the company.

Write a report discussing security vulnerabilities that can lead to the loss of confidentiality, integrity, availability, authenticity, or accountability.

Your well-written paper should meet the following requirements:
- Paper length: 2-3 pages
- Illustrations: Include an illustrative table or a diagram that can be created or included from properly cited external references.
- References: Include two external references in addition to the textbook.
- Format: Follow the CSU-Global APA guidelines.

Option #2: Role of CIA triad in information security
You have been hired to implement a new e-commerce site for a small handmade crafts company with 5 employees. Utilizing the CIA triad, how would you approach security? What should you consider? What could go wrong?

Your well-written paper should meet the following requirements:
- Paper length: 2-3 pages
- Illustrations: Include an illustrative table or a diagram that can be created or included from properly cited external references.
- References: Include two external references in addition to the textbook.
- Format: Follow the CSU-Global APA guidelines.

Module 2

Critical Thinking Assignment (75 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: Network Security Vulnerabilities
You have been subcontracted as an IT consultant by a small bank to prepare a study report about the bank’s potential network security vulnerabilities.

You are charged with the task of pointing out the security threats that should be taken into consideration when a private bank network is established to allow the bank’s customers to perform bank transactions remotely.

Your well-written paper should meet the following requirements:
Option #2: Password Authentication
As companies try to increase the security of their IT infrastructure, the number of password protected areas is growing. Simultaneously, the number of Internet sites which require a username and password combination is also increasing. What are the advantages and disadvantages of password authentication in terms of security, usability, and breadth of support?

Your well-written paper should meet the following requirements:
- Paper length: 2-3 pages
- Illustrations: Include an illustrative table or a diagram that can be created or included from properly cited external references.
- References: Include two external references in addition to the textbook.
- Format: Follow the CSU-Global APA guidelines.

Portfolio Project Milestone #1 (25 points)

Option #1: In 1-2 pages, describe the company you will use for the portfolio submission. Include size, industry, and location.

Option #2: Provide a list of the cases you will explore in detail in your portfolio project, and for each case on your list, explain why the case interests you.

Module 3

Critical Thinking Assignment (75 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: Malware Attacks
You are the information technology manager of a giant hospital that has the capacity of 1000 inpatients. The IT department is responsible for all the hospital technology needs in addition to preserving patients’ records.

One important goal to be achieved is making sure that patients’ records are guarded against any malware attacks. During this process, there is a need for you to write a report assessing the types of possible malware attacks that might affect the hospital information systems.

Your well-written paper assessing the types of possible malware attacks should meet the following requirements:
- Paper length: 2-3 pages
- Illustrations: Include an illustrative table or a diagram that can be created or included from properly cited external references.
- References: Include two external references in addition to the textbook.
Option #2: Malware Attacks

Large scale malware attacks seem to happen with more and more frequency each year. Conduct research to identify a large scale malware attack that occurred within the past 5 years. Provide an overview of the malware, discuss the vulnerability it exploited, how the attack occurred, how many systems were affected, how the exploit was discovered, and lastly how the attack was mitigated and the system restored and protected?

Your well-written paper should meet the following requirements:

- Paper length: 2-3 pages
- Illustrations: Include an illustrative table or a diagram that can be created or included from properly cited external references.
- References: Include two external references in addition to the textbook.
- Format: Follow the CSU-Global APA guidelines.

Module 5

Critical Thinking Assignment (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: Risk Assessment Methodology
You are a senior information technology analyst at your company. Your company has 250 employees. Each employee has his or her own terminal to access the company's network. There are also 10 wireless access points to support access for portable devices.

You have been charged with the task of developing a detailed risk assessment methodology. For this assignment, you should submit a report in which you discuss various risk assessment methodologies, then adopt a methodology and strongly justify your selection.

Your well-written paper should meet the following requirements:

- Paper length: 2-3 pages
- Illustrations: Include an illustrative table or a diagram that can be created or included from properly cited external references.
- References: Include two external references in addition to the textbook.
- Format: Follow the CSU-Global APA guidelines.

Option #2: IT Security Controls
IT security controls are required for many industries and government agencies. There are numerous information security standards and control frameworks available. Conduct research to identify three information security standards. Describe each information security standard. Does it have a target audience? If so, who is the target audience? Compare and contrast the similarities and differences in each standard/framework.

Your well-written paper should meet the following requirements:

- Paper length: 2-3 pages
- Illustrations: Include an illustrative table or a diagram that can be created or included from properly cited external references.
- References: Include two external references in addition to the textbook.
- Format: Follow the CSU-Global APA guidelines.
Module 6

Portfolio Project Milestone #2 (25 points)

**Option #1:** Provide an outline of the security models you will be presenting in your portfolio project.

**Option #2:** Provide a brief description of each case you have chosen for the portfolio project and at least one reference for each case.

**Critical Thinking Assignment (75 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: Physical Security Measures**

You are the IT manager of a small 20-employee technology company that recently won a contract with the Department of Defense. In order to begin work on the contract you must ensure you can protect and safeguard information provided by the government. The company CEO has asked you to prepare a report on the physical security measures you would implement at the company and describe the threats the controls are mitigating against.

Your well-written paper should meet the following requirements:

- Paper length: 2-3 pages
- Illustrations: Include an illustrative table or a diagram that can be created or included from properly cited external references.
- References: Include two external references in addition to the textbook.
- Format: Follow the CSU-Global APA guidelines.

**Option #2: Incident Response Plans**

You are the CIO of a multinational corporation that just opened a 100-employee office in the southeastern US. One of the first steps the CEO wants to take is to ensure that all internal policies and procedures reflect operations at the new location. The CEO has tasked you with developing the company incident response plan. Discuss the role of an incident response plan, major incident response steps, and examples of how the plan can be implemented.

Your well-written paper should meet the following requirements:

- Paper length: 2-3 pages
- Illustrations: Include an illustrative table or a diagram that can be created or included from properly cited external references.
- References: Include two external references in addition to the textbook.
- Format: Follow the CSU-Global APA guidelines.

Module 8

**Portfolio Project Reminder (300 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: Organizational Security Model to Reduce Risks**

You are the information technology senior analyst at your company. Your company can be a real business where you work or a virtual business that you would like to start. In both cases, you should be familiar with the business environment and the nature of work performed at your selected company. If you need help with selecting an appropriate company, please contact your instructor.
Your CEO meets with you and assigns you the following tasks, which you will assemble in a written report to the CEO:

- Review the company's infrastructure and identify all types of vulnerabilities: environmental, physical, and human.
- Suggest and discuss security models that can be used to overcome the associated security risks.
- Design a robust security plan for the company.
- Design a code of ethics related to the IT profession that can be applied at the company.

**Portfolio Milestones:**
You will complete and receive points for two Portfolio Milestones that will help you complete your project. This work will inform your final project, but you will not re-submit this work with your final project. Here are the two milestones:

**Module 2:** Describe the company you will be analyzing for the project. Include size, industry, and location. (25 Points)

**Module 6:** Provide an outline of the security models you will be presenting in your portfolio project. (25 Points)

Your well-written Portfolio Project should meet the following requirements:

- Paper length: 8-10 pages
- Include at least five references in addition to the course textbook. The CSU-Global Library is a good place to find quality resources.
- Format according to CSU-Global APA guidelines.
- When you are ready to submit your project, click the Module 8: Portfolio Project header in the Module 8 folder.
- Do NOT include Milestones 1 and 2 in this submission.

**Option #2: Cybersecurity Breaches and Mitigation**
In the broadest sense, a digital crime is any illegal activity that uses a computer during its commission. Computer crime encompasses a wide range of activities from fraud and financial crimes, cyber terrorism, cyber extortion, to even cyber warfare. Conduct research on 5 different types of digital crime and real-world examples of each. For each real-world example:

- Describe the crime that was committed.
- How was a computer used in the crime?
- Who were the victim(s) of the crime?
- What was the effect or outcome of the criminal act (on the system/victim)?
- How could the crime have been prevented?
- Were the perpetrators identified or caught?
- Was any action taken against the perpetrators, and if so, what?

**Portfolio Milestones:**
You will complete and receive points for two Portfolio Milestones that will help you complete your project. This work will inform your final project, but you will not re-submit this work with your final project.

**Module 2:** Provide an outline of the 5 types of cyber crime you will research. (25 Points)

**Module 6:** Provide the 5 real-world cases you will analyze for the portfolio project. (25 points)

Your well-written paper should meet the following requirements:
- Paper length: 8-10 pages
- Include at least five references in addition to the course textbook. The CSU-Global Library is a good place to find quality resources.
- Format according to CSU-Global APA guidelines.
- When you are ready to submit your project, click the Module 8: Portfolio Project header in the Module 8 folder.
- Do NOT include Milestones 1 and 2 in this submission.

Course Policies

Course Grading

<table>
<thead>
<tr>
<th>Grading Scale and Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>20% Discussion Participation</td>
</tr>
<tr>
<td>8% Mastery Exercises</td>
</tr>
<tr>
<td>37% Critical Thinking Activities</td>
</tr>
<tr>
<td>35% Final Portfolio Paper</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

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 Requirements 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 Requirements 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 on your course’s Assignments page.

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.