Colorado State University GLOBAL CAMPUS

ITS360: INTRODUCTION TO CYBERSECURITY 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.

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 introduction to cyber security and digital crime to students and information technology professionals interested in information security. Students will learn about information security threats, dangers, and risks that organizations face in the workplace as well as gain the ability to analyze potential vulnerabilities that can have an adverse impact on digital assets.

COURSE OVERVIEW:

This course provides an introduction to cyber security and digital crime to students and information technology professionals interested in information security. Students will learn about information security threats, dangers, and risks that organizations face in the workplace as well as gain the ability to analyze potential vulnerabilities that can have an adverse impact on digital assets.

COURSE LEARNING OUTCOMES:

1. Practice 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 enterprise security vulnerabilities at various business sectors.
3. Demonstrate the adverse impact of digital assets that are caused by security vulnerabilities and loss effects.
4. Produce enterprise security needs to determine recommendations for an enterprise technology infrastructure.
5. Apply various security models and measures to an enterprise infrastructure.
6. Compare the benefits gained from applying various security measures to enterprise infrastructure.
7. Summarize the types of computer crime, intellectual property, and codes of ethics that relate to an Information technology professional.

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:

Stallings, W., & Brown, L. (2015). *Computer security: Principles and practice*. Upper Saddle River, NJ: Pearson Education, Inc. ISBN-13:9780133773927

Suggested:

Whitman, M., & Mattord, H. (2018). *Principles of information security*. Independence, KY: Cengage. ISBN – 13: 9781337102063

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.
- **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

- Chapter 1 in *Computer Security: Principles and Practice*

- Kul, G., Upadhyaya, S., & Hughes, A. (2017). Complexity of insider attacks to databases. *ACM International Workshop on Managing Insider Security Threats (MIST)*, 25-32.
- Moriano, P., Pendleton, J., Rich, S., & Camp, L.J. (2017). Insider threat event detection in user-system interactions. *ACM International Workshop on Managing Insider Security Threats (MIST)*, 1-12.

Opening Exercise (0 points)

Discussion (25 points)

Critical Thinking (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: Assessing the Impact Level for the Loss of Confidentiality, Integrity, and Availability

An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

Your paper needs to address and assess the impact (low, moderate, or high) for the loss of confidentiality, integrity, and availability (CIA). Make sure you justify your answers.

Your well-written paper should meet the following requirements:

- Paper length: 2-3 pages
- Include an illustrative table, graphic, or other diagram that can be created or included from properly cited external references.
- Include two external, scholarly references in addition to the textbook. Do not use blogs, wikis, or other non-scholarly sources.
- Format according to CSU-Global APA guidelines.

Option 2: Assessing the Role of CIA Triad in Information Security

A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

Your paper needs to address and assess the impact (low, moderate, or high) for the loss of confidentiality, integrity, and availability (CIA). Make sure you justify your answers.

Your well-written paper should meet the following requirements:

- Paper length: 2-3 pages
- Include an illustrative table, graphic, or other diagram that can be created or included from properly cited external references.
- Include two external, scholarly references in addition to the textbook. Do not use blogs, wikis, or other non-scholarly sources.
- Format according to CSU-Global APA guidelines.

Mastery Exercise (10 points)

MODULE 2

Readings

- Chapter 3 in *Computer Security: Principles and Practice*
- Liang, X., & Kotz, D. (2017). AutoRing: Wearable user-presence authentication. *ACM International Workshop on Wearable Systems and Applications (WearSys)*, 5-10.
- Liu, R., Cornelius, C., Rawassizadeh, R., Peterson, R., & Kotz, D. (2017). Poster: vocal resonance as a passive biometric. *ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 160.

Opening Exercise (0 points)

Discussion (25 points)

Critical Thinking (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: New Authentication Proposal

A relatively new authentication proposal is the Secure Quick Reliable Login (SQRL). It is described at the following link:

- Secure Quick Reliable Login

Briefly summarize how SQRL works and indicate how it fits into the categories of types of user authentication. Provide the benefits and identify any possible security issues with SQRL.

Your well-written paper should meet the following requirements:

- Paper length: 2-3 pages
- Include an illustrative table, graphic, or other diagram that can be created or included from properly cited external references.
- Include two external, scholarly references in addition to the textbook. Do not use blogs, wikis, or other non-scholarly sources.
- Format according to CSU-Global APA guidelines.

Option 2: Password Authentication

Explain why biometric authentication protocols and the biometric capture device are authenticated in the case of static biometric, but not authenticated for a dynamic biometric.

Your well-written paper should meet the following requirements:

- Paper length: 2-3 pages
- Include an illustrative table, graphic, or other diagram that can be created or included from properly cited external references.
- Include two external, scholarly references in addition to the textbook. Do not use blogs, wikis, or other non-scholarly sources.
- Format according to CSU-Global APA guidelines.

Mastery Exercise (10 points)

Portfolio Milestone (25 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

Describe the company you will be analyzing for the project. Include size, industry, and location**.**

Option 2

Provide an outline of the 5 types of cybercrime you will research.

MODULE 3

Readings

- Chapter 6 in *Computer Security: Principles and Practice*
- Nicholas, C. (2017). Document engineering issues in malware analysis. *ACM International Symposium on Documents Engineering (DocEng)*, 3.
- Sinanovic, H., & Mrdovic, S. (2017). Analysis of mirai malicious software. *IEEE International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, 1-5. Retrieved from http://people.etf.unsa.ba/~smrdovic/publications/SoftCOM2017_Sinanovic_Mrdovic.pdf
- Yang, W., Kong, D., Xie, T., & Gunter, C. (2017). Malware detection in adversarial settings: Exploiting feature evolutions and confusions in Android apps. *ACM International Conference on Security Applications Conference (ACSAC)*, 288-302.

Opening Exercise (0 points)

Discussion (25 points)

Mastery Exercise (10 points)

Critical Thinking (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: Identifying Malicious Software

Assume you have found a USB memory stick in your work parking area. What threats might this pose to your work computer should you just plug the memory stick in and examine its content? In particular, consider whether each of the malware propagation mechanisms we discuss could use such a memory stick for transport. What steps could you take to mitigate these threats, and safely determine the contents of the memory stick? Support your answers by surveying various malware and how they affect systems and users.

Your well-written paper should meet the following requirements:

- Paper length: 2-3 pages
- Include an illustrative table, graphic, or other diagram that can be created or included from properly cited external references.
- Include two external, scholarly references in addition to the textbook. Do not use blogs, wikis, or other non-scholarly sources.
- Format according to CSU-Global APA guidelines

Option 2: Malware Attacks

Suppose that while trying to access a collection of short videos on some Web site, you see a pop-up window stating that you need to install this custom codec in order to view the videos. What threat

might this pose to your computer system if you approve this installation request? Support your answers by surveying various malware and how they affect systems and users.

Your well-written paper should meet the following requirements:

- Paper length: 2-3 pages
- Include an illustrative table, graphic, or other diagram that can be created or included from properly cited external references.
- Include two external, scholarly references in addition to the textbook. Do not use blogs, wikis, or other non-scholarly sources.
- Format according to CSU-Global APA guidelines.

MODULE 4

Readings

- Chapter 14 in *Computer Security: Principles and Practice*
- Laube, S., & Bohme, R. (2017). Strategic aspects of cyber risks information sharing. *ACM Computing Survey (CSUR), 50(5)*, 1-36.
- Suroso, J., & Rahadi, D. (2017). Development of IT risk management framework using COBIT 4.1, implementation in IT governance for support business strategy. *ACM International Conference on Education and Multimedia Technology (ICEMT)*, 92-96.

Opening Exercise (0 points)

Discussion (25 points)

Mastery Exercise (10 points)

MODULE 5

Readings

- Chapter 15 in *Computer Security: Principles and Practice*
- Ceccheti, E., Myers, A., & Arden, O. (2017). Nonmalleable information flow control. *ACM International Conference on Computer and Communications Security (SIGSAC)*, 1875-1891.
- Dunets, O., Wolff, C., Sachenko, A., Hladiy, G., & Dobrotvor, I. (2017). Multi-agent system of IT project planning. *IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, 548-552. Retrieved from http://idaacs.net/storage/conferences/2/abstracts/i17-161-056005bff6d3a30e356d4176811359b5.doc
- Olagunju, A., Franske, B., & Silman, D. (2017). MySecurityLab: A generic tool for self-paced learning of security controls. *ACM International Conference on Information Technology Education (SIGITE)*, 67.

Opening Exercise (0 points)

Discussion (25 points)

Mastery Exercise (10 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: Understanding Risk Assessment Methodology

Consider the risk to "integrity of customer and financial data files on system" from "corruption of these files due to import of a worm/virus onto a system," as discussed in Problem 14.2 in your textbook. From the list shown in Table 15.3 in your textbook, select some suitable specific controls that could reduce this risk. Indicate which you believe would be most cost effective. Support your answers with references.

Your well-written paper should meet the following requirements:

- Paper length: 2-3 pages
- Include an illustrative table, graphic, or other diagram that can be created or included from properly cited external references.
- Include two external, scholarly references in addition to the textbook. Do not use blogs, wikis, or other non-scholarly sources.
- Format according to CSU-Global APA guidelines.

Option 2: Understanding IT Security Controls

Consider the risk to "integrity of the accounting records on the server" from "corruption of these files due to import of a worm/virus onto a system," as discussed in Problem 14.3 in your textbook. From the list shown in Table 15.3 in your textbook, select some suitable specific controls that could reduce this risk. Indicate which you believe would be most cost effective. Support your answers.

Your well-written paper should meet the following requirements:

- Paper length: 2-3 pages
- Include an illustrative table, graphic, or other diagram that can be created or included from properly cited external references.
- Include two external, scholarly references in addition to the textbook. Do not use blogs, wikis, or other non-scholarly sources.

  Format according to CSU-Global APA guidelines.

MODULE 6

Readings

- Chapter 16 in *Computer Security: Principles and Practice*
- Google Cloud (2017). Google infrastructure security design overview. Retrieved from https://cloud.google.com/security/security-design/resources/google_infrastructure_whitepaper_fa.pdf
- Shabtai, A., & Elovici, Y. (2014). Misuseability analysis for IT infrastructure. *ACM International Conference on Computer and Communications Security (SIGSAC)*, 1496-1498.

Opening Exercise (0 points)

Discussion (25 points)

Mastery Exercise (10 points)

Critical Thinking (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

Write a detailed report on the four protected area types described in the NIST SP 800-116.

Your well-written paper should meet the following requirements:

- Paper length: 2-3 pages
- Include an illustrative table, graphic, or other diagram that can be created or included from properly cited external references.
- Include two external, scholarly references in addition to the textbook. Do not use blogs, wikis, or other non-scholarly sources.
- Format according to 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
- Include an illustrative table, graphic, or other diagram that can be created or included from properly cited external references.
- Include two external, scholarly references in addition to the textbook. Do not use blogs, wikis, or other non-scholarly sources.
- Format according to CSU-Global APA guidelines.

Portfolio Milestone (25 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

Provide an outline of the security models you will be presenting in your portfolio project.

Option 2

Provide the 5 real-world cases you will analyze for the portfolio project.

MODULE 7

Readings

- Chapter 17 in *Computer Security: Principles and Practice*
- Katsantonis, M., Fouliras, P., & Mavridis, I. (2017). Conceptualization of game based approaches for learning and training on cyber security. *ACM International Conference on Informatics (PCI)*, 1-2.
- Wen, Z., Li, Y., Wade, R., Huang, J., & Wang, A. (2017). What.hack: Learn phishing email defense the fun way. *ACM International Conference on Human Factors in Computing Systems (CHI EA)*, 234-237.

Opening Exercise (0 points)

Discussion (25 points)

Mastery Exercise (10 points)

MODULE 8

Readings

- Chapter 19 in *Computer Security: Principles and Practice*
- Andrews, C. (2017). Cyber car crime: Thieves turn to high tech [transport car crime]. *IET Journal of Engineering & Technology*, *12*(2), 32-35. Retrieved from https://eandt.theiet.org/content/articles/2017/02/cyber-car-crime-thieves-turn-to-high-tech/
- Mazurczyk, W., Holt, T., & Szczypiorski, K. (2017). Guest editors' introduction: Special issue on cyber crime. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 146-147. Retrieved from https://www.computer.org/csdl/trans/tq/2016/02/07430415.pdf
- Misyrlis, M., Cheung, C., Srivastava, A., Kannan, R., & Prasanna, V. (2017). Spatio-temporal modeling of criminal activity. *ACM International Workshop on Social Sensing (SocialSens)*, 3-8.
- Vardi, M. (2017). Cyber insecurity and cyber libertarianism. Communication of the *ACM, 60(5)*, 1.

Opening Exercise (0 points)

Discussion (25 points)

Mastery Exercise (10 points)

Portfolio Project (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: Information Technology Analysis

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 of 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 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 paper should meet the following requirements:

- Paper length: 8-10 pages
- Include at least five scholarly references in addition to the course textbook. The CSU-Global Library is a good place to find these references.
- Format according to CSU-Global APA guidelines.

Option 2: Digital Crime

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 cybercrime 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 scholarly references in addition to the course textbook. The CSU-Global Library is a good place to find these references.
- Format according to CSU-Global APA guidelines.

COURSE POLICIES

Course Grading

20% Discussion Participation
0% Opening Exercises
0% Live Classroom
8% Mastery Exercises
37% Critical Thinking Assignments
35% Final Portfolio Project

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

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 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 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.