Course Description

Introduces the types of security crime, breaches, fraud, and network penetrations. Students learn procedures for preventing intrusions, fraud, and computer crime. Legal impacts for cyber security crimes are discussed and evaluated.

Course Textbook


Course Learning Outcomes

Upon completion of this course, students should be able to:

1. Explain the relevance of cyber security.
2. Identify the types of cybercrime.
3. Update computer security and firewall settings.
4. Scan for malware, rootkits, and malicious software.
5. Configure browser settings, data execution prevention, and local security policy.
6. Utilize EULA analyzer, port scanners, network protocol analyzers, and key logger software.
7. Analyze security risks and traffic.
8. Identify legal sanctions for cybercrime.
9. List the procedures for a disaster recovery plan.
10. Explain the importance of security training and awareness.
11. Compare cloud computing features.

Credits

Upon completion of this course, the students will earn three (3) hours of college credit.

Course Structure

1. **Study Guide**: Each unit contains a Study Guide that provides students with the learning outcomes, unit lesson, required reading assignments, and supplemental resources.
2. **Learning Outcomes**: Each unit contains Learning Outcomes that specify the measurable skills and knowledge students should gain upon completion of the unit.
3. **Unit Lesson**: Each unit contains a Unit Lesson, which discusses lesson material.
4. **Reading Assignments**: Each unit contains Reading Assignments from one or more chapters from the textbook. Chapter presentations are provided in the Unit I-II and IV-VIII study guides as Required Reading to aid students in their course of study.
5. **Suggested Reading**: Suggested Readings are listed in Units I-IV and VI-VII. Students are encouraged to read the resources listed if the opportunity arises, but they will not be tested on their knowledge of the Suggested Readings.
6. **Learning Activities (Non-Graded)**: These non-graded Learning Activities are provided to aid students in their course of study.
7. **Unit Assessments**: This course contains one Unit Assessment, to be completed at the end of Unit VII. The Assessment is composed of written-response questions.
8. **Unit Assignments**: Students are required to submit for grading Unit Assignments in each unit. Specific information and instructions regarding these assignments are provided below. Grading rubrics are included with each assignment. Specific information about accessing these rubrics is provided below.
9. **Ask the Professor:** This communication forum provides you with an opportunity to ask your professor general or course content related questions.

10. **Student Break Room:** This communication forum allows for casual conversation with your classmates.

### CSU Online Library

The CSU Online Library is available to support your courses and programs. The online library includes databases, journals, e-books, and research guides. These resources are always accessible and can be reached through the library webpage. To access the library, log into the myCSU Student Portal, and click on “CSU Online Library.” You can also access the CSU Online Library from the “My Library” button on the course menu for each course in Blackboard.

The CSU Online Library offers several reference services. E-mail (library@columbiasouthern.edu) and telephone (1.877.268.8046) assistance is available Monday – Thursday from 8 am to 5 pm and Friday from 8 am to 3 pm. The library’s chat reference service, Ask a Librarian, is available 24/7; look for the chat box on the online library page.

Librarians can help you develop your research plan or assist you in finding relevant, appropriate, and timely information. Reference requests can include customized keyword search strategies, links to articles, database help, and other services.

### Security Tools Use and Applications

Cautionary note: Please read your book, and do not just scan the readings. Read your announcements and this syllabus for potential changes to assignments, non-working links, etc. The tools used in this class and the course layout allow the student to engage in hands-on discovery of information and information gathering and to assess vulnerabilities. An ethical hacker follows the book and syllabus. At no time are you actually conducting a penetration of a website or network to disrupt or gather sensitive information. You are being exposed to the basic tools that a hacker uses to discover and gather information to attack or penetrate a website or network for criminal purposes. Most of these tools are used today by systems administrators to gather information on how to protect and secure an organization’s network and systems.

You must use your own laptop or desktop computer in which you have administrative rights and not a public computer (used at your organization or workplace, a library, etc.). Those computer systems that do not belong to you personally will not grant you certain administrative rights to view download, upload, or Internet search information. Please see your student handbook on required technology requirements.

### Unit Assignments

#### Unit I PowerPoint Presentation

Create a 7-10-slide PowerPoint Presentation on the challenges of securing information, and list some of today’s information security attacks. You may use various sources (scholarly), but at a minimum, your textbook must be used. Be sure to cite any sources used in a reference slide with proper APA formatting. (Title and reference slides do not count in the total number of slides).

Information about accessing the Blackboard Grading Rubric for this assignment is provided below.

#### Unit I Reflection Paper

The primary tenets of information security are represented by the triad “C-I-A.” Discuss the importance and impact of each of the tenets as they relate to an organization’s data. Is there one tenet that is more important than another? Explain.

Your response should be at least 200 words in length. You are required to use at least your textbook as source material for your response. All sources used, including textbook, must be referenced; paraphrased and quoted material must have accompanying citations.

Information about accessing the Blackboard Grading Rubric for this assignment is provided below.
Unit II Scholarly Activity

At the end of Chapter 2 in your textbook, you will find a list of Case Projects. Select one of the following Case Projects and prepare a one-two-page paper.

- Case Project 2-1: Researching Virus Attacks
- Case Project 2-2: Researching Social Engineering
- Case Project 2-3: Fighting Spam
- Case Project 2-4: Defining Spyware

Use your own words, and remember to apply APA style to your paper.

Information about accessing the Blackboard Grading Rubric for this assignment is provided below.

Unit II Assignment

For this assignment, select ONE of the following options:

**Option One:** In this web research project, identify at least four types of cybercrimes. Using at least two sources on the Internet, briefly research cybercrimes, and write a one-page (250-word) paper. Use APA style to format your paper, including double spacing, citations, and references.

**Option Two:** This option asks you to prepare a PowerPoint Presentation describing at least four social-engineering attacks. Using at least two sources on the Internet, examine and differentiate among the types of social engineering attacks. Create a 10-12-slide presentation, and include the following in your presentation:

- Introductory slide
- Content slides
- Closing slide

Be sure to properly cite any sources you use for your presentation. Add presenter’s notes that include talking points and details to each slide of the presentation.

CSU requires that students use the APA style for papers and projects. Therefore, the APA rules for formatting, quoting, paraphrasing, citing, and listing of sources are to be followed.

Information about accessing the Blackboard Grading Rubric for this assignment is provided below.

Unit III Web Assignment

In this assignment, you will research and identify one of the laws that governs computer access and trespass. Begin by selecting ONE of the following governances, laws, or standards:

1. The USA Patriot Act of 2001:
   [http://www.justice.gov/archive/ll/highlights.htm](http://www.justice.gov/archive/ll/highlights.htm)

2. The Computer Fraud and Abuse Act:

3. The Electronic Communications Privacy Act:

4. The Payment Card Industry Data Security Standard:

5. Health Insurance Portability and Accountability Act:

6. Another governance, law, or standard of your choosing.
After conducting research online, write a two-page (500-word) paper. Within the paper, include each of the following:

1. Provide an overview of the governance, law, or standard explaining how it is intended to protect civilians.
2. Does adhering to the governance, law, or standard include any nuisances? Does it place a hardship on users or organizations? List them.
3. Describe an example scenario where the governance, law, or standard is violated (this can be real or fictitious).
4. Provide your own thoughts about the effectiveness of the governance, law, or standard. Does it actually accomplish its intentions?
5. Two references (websites, the CSU Online Library, or books)

Apply APA style to the paper, including in-text citations, references, and the format of the pages.

The purpose of this assignment is to allow you to examine a law or standard that governs computer access and trespass. While this assignment does not allow you to examine all of the laws and standards, it does allow you to utilize the process of researching laws and standards. Thus, it reinforces a technique you can utilize as a life-long learner as well as a professional.

Information about accessing the Blackboard Grading Rubric for this assignment is provided below.

Unit III Reflection Paper

For this reflection paper, you are asked to place yourself in the shoes of a cybersecurity professional by considering the following scenario: Sarah just finished her degree in information technology, and throughout the program, she focused on cybersecurity. That is her specialty as well as her passion. With Sarah’s credentials and her expertise, she is highly sought after by several “A-list” corporations. Sarah is your friend, and she comes to you for advice. She is not sure which corporation she wants to work for because she never thought about it until now. If you could recommend one type of corporation, which one would it be, and which laws should Sarah begin to examine?

Prepare a 150-word response, and be sure to address at least one law related to the corporation’s operations and why it would be an interesting fit for Sarah.

The purpose of this exercise is to allow you to examine the laws as they would apply in a workplace setting.

Information about accessing the Blackboard Grading Rubric for this assignment is provided below.

Unit IV Web Assignment

For this assignment, choose ONE of the following options:

Option 1: Conduct research on the Internet, and write a one-two-page paper on some of the highly publicized DoS attacks that have occurred most recently. Include in your paper the attackers who launch these attacks, and discuss how these attacks can be prevented. Include a title page and separate references page. Follow CSU APA guidelines. This includes in-text citations, referencing, and formatting of the pages.

Option 2: Conduct research on the Internet and write a one-two-page paper on how zero day attack vulnerabilities are discovered. Include in the paper some of the most recent zero day attacks. Also, describe how to defend against zero day attacks. Include a title page and separate references page. Follow CSU APA guidelines. This includes in-text citations, referencing, and formatting of the pages.

Information about accessing the Blackboard Grading Rubric for this assignment is provided below.

Unit V Assignment

This assignment asks you to participate in two projects and then to write about both projects in ONE paper.

1. Complete Project 4-1: Using an Internet Port Scanner on page 150 within the textbook
2. Complete Project 4-4: Launching the Linux Wireshark Network Protocol Analyzer on pages 154-156 within the textbook

Write a one-two-page paper about both projects, and describe any unusual problems that arose as a result of these projects. Also include a brief description of a port scanner and a network protocol analyzer. Include a title page and a
separate reference page. Follow CSU APA guidelines. This includes in-text citations, referencing and formatting of the paper.

Information about accessing the Blackboard Grading Rubric for this assignment is provided below.

Unit V Reflection Paper

Research the mobile device security that is available for different smartphones. Then explain which one you would recommend. Why? Prepare at least a 250-word response, and please cite your work with references.

Information about accessing the Blackboard Grading Rubric for this assignment is provided below.

Unit VI Assignment

This assignment asks you to participate in three projects and then to write about each project in one paper. Begin by following the instructions for each project provided within the textbook.

1. Case Project 6-4: Network Firewall Comparison on page 247 within the textbook
2. Case Project 7-2: Comparing Cloud Computing Features on page 288 within the textbook
3. Project 1-3: Use an Eula Analyzer on pages 34-35 within the textbook

Note: For Project 1-3, the first hyperlink is broken (www.microsoft.com/About/Legal/EN/US/IntellectualProperty/UseTerms/Default.aspx), so use the following hyperlink in its place: https://www.microsoft.com/en-us/useterms

Write a two-page paper following the directions within the textbook on Case Project 6-4, Case Project 7-2, and Project 1-3. Include a title page and separate reference page. Follow CSU APA Guidelines, including in-text citations, referencing, and formatting of the paper.

Information about accessing the Blackboard Grading Rubric for this assignment is provided below.

Unit VI Reflection Paper

For this reflection paper, draft a 250-word response to the following question: What are some security concerns with virtualized networks? Do you feel that a virtualized network is secure enough to host identity information (i.e., social security number, etc.)? Why, or why not?

Please cite your work with references by using APA style.

Information about accessing the Blackboard Grading Rubric for this assignment is provided below.

Unit VII Reflection Paper

Is car hacking a reality or a myth? Here is a short clip from the movie After the Sunset (http://youtu.be/vglNcqT3VE)—can this really happen? From an authentication perspective, what can you do to help prevent car hacking from occurring? This exercise asks you to think critically about the authentication and account management concepts in this unit and then apply them to a potential threat such as car hacking.

Prepare at least a 250-word response, and please cite your work with references. You may use the Internet to support your response.

Information about accessing the Blackboard Grading Rubric for this assignment is provided below.

Unit VIII PowerPoint Presentation

Create a five-seven- PowerPoint Presentation on what goes in to a disaster recovery plan. Include all the units as outlined in the textbook, and explain each section of the plan. Be sure to cite any sources used in a reference slide with proper APA formatting. (The cover and reference slides do not contribute to the slide count). You may also use the slide notes function to explain slide content as necessary.

Information about accessing the Blackboard Grading Rubric for this assignment is provided below.
Ciampa (2012) discusses training techniques in Chapter 14. Why is it important to train employees about security defenses? Does training employees increase or decrease security for an organization? Explain. There is not a right or wrong answer to this question. Use your critical thinking skills to examine how training employees can impact the overall security of an organization.

Information about accessing the Blackboard Grading Rubric for this assignment is provided below.

**APA Guidelines**

The application of the APA writing style shall be practical, functional, and appropriate to each academic level, with the primary purpose being the documentation (citation) of sources. CSU requires that students use APA style for certain papers and projects. Students should always carefully read and follow assignment directions and review the associated grading rubric when available. Students can find CSU’s Citation Guide by clicking [here](#). This document includes examples and sample papers and provides information on how to contact the CSU Success Center.

**Grading Rubrics**

This course utilizes analytic grading rubrics as tools for your professor in assigning grades for all learning activities. Each rubric serves as a guide that communicates the expectations of the learning activity and describes the criteria for each level of achievement. In addition, a rubric is a reference tool that lists evaluation criteria and can help you organize your efforts to meet the requirements of that learning activity. It is imperative for you to familiarize yourself with these rubrics because these are the primary tools your professor uses for assessing learning activities.

Rubric categories include: (1) Assessment (Written Response) and (2) Assignment. However, it is possible that not all of the listed rubric types will be used in a single course (e.g., some courses may not have Assessments).

The Assessment (Written Response) rubric can be found embedded in a link within the directions for each Unit Assessment. However, these rubrics will only be used when written-response questions appear within the Assessment.

Each Assignment type (e.g., article critique, case study, research paper) will have its own rubric. The Assignment rubrics are built into Blackboard, allowing students to review them prior to beginning the Assignment and again once the Assignment has been scored. This rubric can be accessed via the Assignment link located within the unit where it is to be submitted. Students may also access the rubric through the course menu by selecting “Tools” and then “My Grades.”

Again, it is vitally important for you to become familiar with these rubrics because their application to your Assessments and Assignments is the method by which your instructor assigns all grades.

**Communication Forums**

These are non-graded discussion forums that allow you to communicate with your professor and other students. Participation in these discussion forums is encouraged, but not required. You can access these forums with the buttons in the Course Menu. Instructions for subscribing/unsubscribing to these forums are provided below.

Once you have completed Unit VIII, you MUST unsubscribe from the forum; otherwise, you will continue to receive e-mail updates from the forum. You will not be able to unsubscribe after your course end date.

[Click here for instructions on how to subscribe/unsubscribe and post to the Communication Forums](#).

**Ask the Professor**

This communication forum provides you with an opportunity to ask your professor general or course content questions. Questions may focus on Blackboard locations of online course components, textbook or course content elaboration, additional guidance on assessment requirements, or general advice from other students.

Questions that are specific in nature, such as inquiries regarding assessment/assignment grades or personal accommodation requests, are NOT to be posted on this forum. If you have questions, comments, or concerns of a
non-public nature, please feel free to email your professor. Responses to your post will be addressed or emailed by the professor within 48 hours.

Before posting, please ensure that you have read all relevant course documentation, including the syllabus, assessment/assignment instructions, faculty feedback, and other important information.

**Student Break Room**

This communication forum allows for casual conversation with your classmates. Communication on this forum should always maintain a standard of appropriateness and respect for your fellow classmates. This forum should NOT be used to share assessment answers.

**Grading**

<table>
<thead>
<tr>
<th>Component</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit VII Assessment</td>
<td>6%</td>
</tr>
<tr>
<td>PowerPoint Presentations (2 @ 6%)</td>
<td>12%</td>
</tr>
<tr>
<td>Reflection Papers (6 @ 6%)</td>
<td>36%</td>
</tr>
<tr>
<td>Unit II Scholarly Activity</td>
<td>8%</td>
</tr>
<tr>
<td>Unit II Assignment</td>
<td>10%</td>
</tr>
<tr>
<td>Unit V and VI Assignments (2 @ 6%)</td>
<td>12%</td>
</tr>
<tr>
<td>Web Assignments (2 @ 8%)</td>
<td>16%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

**Course Schedule/Checklist (PLEASE PRINT)**

The following pages contain a printable Course Schedule to assist you through this course. By following this schedule, you will be assured that you will complete the course within the time allotted.
# CYB 4301, Cyber Security and Crime

## Course Schedule

By following this schedule, you will be assured that you will complete the course within the time allotted. Please keep this schedule for reference as you progress through your course.

<table>
<thead>
<tr>
<th>Unit I</th>
<th>Introduction to Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review:</td>
<td></td>
</tr>
<tr>
<td>□ Unit Study Guide</td>
<td></td>
</tr>
<tr>
<td>□ Learning Activities (Non-Graded): See Study Guide</td>
<td></td>
</tr>
<tr>
<td>Read:</td>
<td></td>
</tr>
<tr>
<td>□ Chapter 1: Introduction to Security</td>
<td></td>
</tr>
<tr>
<td>□ Additional Reading Assignment(s): See Study Guide</td>
<td></td>
</tr>
<tr>
<td>□ Suggested Reading: See Study Guide</td>
<td></td>
</tr>
<tr>
<td>Submit:</td>
<td></td>
</tr>
<tr>
<td>□ PowerPoint Presentation</td>
<td></td>
</tr>
<tr>
<td>□ Reflection Paper</td>
<td></td>
</tr>
</tbody>
</table>

Notes/Goals:

<table>
<thead>
<tr>
<th>Unit II</th>
<th>Malware and Social Engineering Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review:</td>
<td></td>
</tr>
<tr>
<td>□ Unit Study Guide</td>
<td></td>
</tr>
<tr>
<td>□ Learning Activities (Non-Graded): See Study Guide</td>
<td></td>
</tr>
<tr>
<td>Read:</td>
<td></td>
</tr>
<tr>
<td>□ Chapter 2: Malware and Social Engineering Attacks</td>
<td></td>
</tr>
<tr>
<td>□ Additional Reading Assignment(s): See Study Guide</td>
<td></td>
</tr>
<tr>
<td>□ Suggested Reading: See Study Guide</td>
<td></td>
</tr>
<tr>
<td>Submit:</td>
<td></td>
</tr>
<tr>
<td>□ Scholarly Activity</td>
<td></td>
</tr>
<tr>
<td>□ Assignment</td>
<td></td>
</tr>
</tbody>
</table>

Notes/Goals:

<table>
<thead>
<tr>
<th>Unit III</th>
<th>The Legal Aspects of Electronic Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review:</td>
<td></td>
</tr>
<tr>
<td>□ Unit Study Guide</td>
<td></td>
</tr>
<tr>
<td>□ Learning Activities (Non-Graded): See Study Guide</td>
<td></td>
</tr>
<tr>
<td>Read:</td>
<td></td>
</tr>
<tr>
<td>□ Chapter 1: Introduction to Security, p. 18</td>
<td></td>
</tr>
<tr>
<td>□ Additional Reading Assignment(s): See Study Guide</td>
<td></td>
</tr>
<tr>
<td>□ Suggested Reading: See Study Guide</td>
<td></td>
</tr>
<tr>
<td>Submit:</td>
<td></td>
</tr>
<tr>
<td>□ Web Assignment</td>
<td></td>
</tr>
<tr>
<td>□ Reflection Paper</td>
<td></td>
</tr>
</tbody>
</table>

Notes/Goals:
<table>
<thead>
<tr>
<th>Unit IV</th>
<th>Application and Network Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Review:</strong></td>
<td>• Unit Study Guide</td>
</tr>
<tr>
<td></td>
<td>• <strong>Learning Activities</strong> (Non-Graded): See Study Guide</td>
</tr>
<tr>
<td><strong>Read:</strong></td>
<td>• Chapter 3: Application and Network Attacks</td>
</tr>
<tr>
<td></td>
<td>• <strong>Additional Reading Assignment(s):</strong> See Study Guide</td>
</tr>
<tr>
<td></td>
<td>• <strong>Suggested Reading:</strong> See Study Guide</td>
</tr>
<tr>
<td><strong>Submit:</strong></td>
<td>• Web Assignment</td>
</tr>
<tr>
<td><strong>Notes/Goals:</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unit V</th>
<th>Vulnerability Assessment and Mitigating Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Review:</strong></td>
<td>• Unit Study Guide</td>
</tr>
<tr>
<td></td>
<td>• <strong>Learning Activities</strong> (Non-Graded): See Study Guide</td>
</tr>
<tr>
<td><strong>Read:</strong></td>
<td>• Chapter 4: Vulnerability Assessment and Mitigating Risks</td>
</tr>
<tr>
<td></td>
<td>• Chapter 5: Host, Application, and Data Security</td>
</tr>
<tr>
<td></td>
<td>• <strong>Additional Reading Assignment(s):</strong> See Study Guide</td>
</tr>
<tr>
<td><strong>Submit:</strong></td>
<td>• Assignment</td>
</tr>
<tr>
<td></td>
<td>• Reflection Paper</td>
</tr>
<tr>
<td><strong>Notes/Goals:</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unit VI</th>
<th>Network Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Review:</strong></td>
<td>• Unit Study Guide</td>
</tr>
<tr>
<td><strong>Read:</strong></td>
<td>• Chapter 6: Network Security</td>
</tr>
<tr>
<td></td>
<td>• Chapter 7: Administering a Secure Network</td>
</tr>
<tr>
<td></td>
<td>• <strong>Additional Reading Assignment(s):</strong> See Study Guide</td>
</tr>
<tr>
<td></td>
<td>• <strong>Suggested Reading:</strong> See Study Guide</td>
</tr>
<tr>
<td><strong>Submit:</strong></td>
<td>• Assignment</td>
</tr>
<tr>
<td></td>
<td>• Reflection Paper</td>
</tr>
<tr>
<td><strong>Notes/Goals:</strong></td>
<td></td>
</tr>
</tbody>
</table>
## Unit VII
### Wireless Network Security, Access Control Models, and Authentication

**Review:**
- ✔️ Unit Study Guide

**Read:**
- ✔️ Chapter 8: Wireless Network Security
- ✔️ Chapter 9: Access Control Fundamentals
- ✔️ Chapter 10: Authentication and Account Management
- ✔️ Additional Reading Assignment(s): See Study Guide
- ✔️ Suggested Reading: See Study Guide

**Submit:**
- ✔️ Assessment
- ✔️ Reflection Paper

---

## Unit VIII
### Business Continuity and Risk Mitigation

**Review:**
- ✔️ Unit Study Guide
- ✔️ Learning Activities (Non-Graded): See Study Guide

**Read:**
- ✔️ Chapter 13: Business Continuity
- ✔️ Chapter 14: Risk Mitigation
- ✔️ Additional Reading Assignment(s): See Study Guide

**Submit:**
- ✔️ PowerPoint Presentation
- ✔️ Reflection Paper

---

Notes/Goals: