

SYLLABUS

CYSA 520 – 740

Fall-B 2021

(Reading Time ~ 11 minutes 34 seconds)

Course Description

CYSA 520 PRINCIPLES OF CYBERSECURITY FOR DATA ANALYTICS (3). A study of cybersecurity to support the principles of confidentiality, integrity, and availability as it applies to data analytics. Topics include evaluating system configurations, performing threat analysis, designing risk mitigation techniques, and understanding applicable policies, laws, and regulations.

Class Meetings

This is a web class and there are no regularly scheduled class meetings.

Instructor

Dr. Mark Ciampa, #228 Grise Hall, mark.ciampa@wku.edu

I am a Professor of Computer Information Systems at Western Kentucky University in Bowling Green, Kentucky and hold a PhD from Indiana State University in Digital Communication Systems. Prior to this I was an Associate Professor and served as the Director of Academic Computing at Volunteer State Community College in Gallatin, Tennessee for 20 years. I have worked in the IT industry as a computer consultant for the U.S. Postal Service, the Tennessee Municipal Technical Advisory Service, and the University of Tennessee. I have also written over 30 college technology textbooks, including *CompTIA CySA+ Guide to Cybersecurity Analyst 2e*, *CWNA Guide to Wireless LANs 3ed*, *Guide to Wireless Communications*, *Security+ Guide to Network Security Fundamentals 7e*, *Security Awareness: Applying Practical Security in Your World 5e*, and *Networking BASICS*.

Office Hours

In-person office hours are posted on my office door. However, due to COVID-19 online virtual office hours will also be offered through Zoom. My virtual office hours will be Monday 9:30 AM – 2:00 PM and Wednesday 1:00 PM – 4:00 PM. If you wish to meet with me, you must send to me an email message at least 24 hours in advance with the date and time you are requesting a meeting. If there is not a meeting already scheduled with another student, then I will send back to you a Zoom link for that meeting. If there is a conflict, I will alert you so that an alternative time can be arranged between us.

Required Materials

The required material is Cengage MindTap for *CompTIA Security+ 7e* (ISBN 9780357640982). The electronic version of the textbook (eBook) is included in the MindTap platform so there is no need to purchase a separate print textbook. See the document “Purchasing Required Materials” under START HERE FIRST on our Blackboard course site. Another purchasing option is to purchase *Cengage Unlimited* that gives access to all Cengage materials. Visit www.cengage.com for more information.

Activities

Below is a summary list of the course activities that you will perform (see the document “Course Activities” on Blackboard for more detailed information)

1. *Complete Course Orientation Activities*
2. *Read Textbook Modules* - You will read two textbook modules (chapters) each week
3. *Perform Module Activities* – You will complete activities and live virtual machine labs that accompany each module.
4. *Take Module Quiz* – There is a quiz for each module and can only be taken once.
5. *Engage in Reflection Discussion* – You will make postings to a discussion activity and interact with other students.
6. *Take Final Exam*

Students may discuss any aspect of a grade received for up to seven (7) calendar days after the grade is posted. After this deadline the grade can no longer be reviewed.

Deadlines

The initial discussion posting deadline is Friday at 8:00 AM for that week; all other weekly assignments must be completed and submitted by Monday at 8:00 AM for that week. No late assignments are accepted. A link to an online course calendar is also on Blackboard.

Grading Percentages

Event	Percentage
Module Activities	60%
Discussions	10%
Final Exam	30%

Grading Scale

Percentage	Letter Grade
90-100%	A
80-89%	B
70-79%	C
60-69%	D
0-59%	F
Other	I (Incompletes are handled on a case-by-case basis)

Grading Principles

1. Students will **not** be allowed to turn in assignments after the deadline has passed.
2. Students will **not** be allowed to “re-do” assignments after they have been graded.

Withdrawal Dates

- October 24 - Last day to withdraw and receive a “No Grade”
- November 17 - Last day to withdraw and receive a grade of “W”

Email

Throughout the semester emails will be sent to the WKU email account of students. You are responsible reading these messages. Because of the number of classes that I’m teaching the volume of emails that I receive from students email messages must be filtered. In order for your messages from this class to be filtered properly and receive my top attention it is required that the subject line of your email is as follows: CYSA 520 – Your Name – Topic of Message (*CIS 205 – Pia Romanelli – Quiz 2 Question*). Under normal circumstances I will respond no later than 24 hours after receiving your email IF it has this subject line; email messages without this subject line may be returned to you or not be answered promptly.

Course Outline

Module 1, “Introduction to Security,” introduces the cybersecurity fundamentals that form the basis of the Security+ certification. The module begins by defining information security and identifying attackers. It also looks at vulnerabilities in systems and the types of attacks that take advantage of the vulnerabilities.

Module 2, “Threat Management and Cybersecurity Resources,” looks at threat management as it pertains to penetration testing and vulnerability scans. The module also explores cybersecurity standards, regulations, frameworks, and configuration guidelines.

Module 3, “Threats and Attacks on Endpoints,” focuses on network-connected hardware devices, better known as endpoints. It begins by looking at attacks using various types of malware and then surveys application attacks. It also examines adversarial artificial intelligence attacks.

Module 4, “Endpoint and Application Development Security,” describes different sources of threat intelligence information. The module also explores securing endpoint devices and creating and deploying secure applications to run on those devices.

Module 5, “Mobile, Embedded, and Specialized Device Security,” looks at securing mobile devices. As users have embraced mobile devices, so too have attackers embraced them as targets. This module also explores embedded systems and the Internet of Things devices. Finally, it examines keeping specialized devices secure.

Module 6, “Basic Cryptography,” explores how encryption can be used to protect data. The module covers what cryptography is and how it can be used for protection, and then examines how to protect data using three common types of encryption algorithms: hashing, symmetric encryption, and asymmetric encryption. It also covers how to use cryptography on files and disks to keep data secure.

Module 7, “Public Key Infrastructure and Cryptographic Protocols,” examines how to implement cryptography and use digital certificates. It also looks at public key infrastructure and key management. This module covers cryptographic protocols to see how cryptography is used on data that is being transported and concludes with how to implement cryptography.

Module 8, “Networking Threats, Assessments, and Defenses,” begins a study of network attacks and defenses. First the module explores some of the common attacks that are launched against networks

today. Then it looks at tools for assessing and defending networks. Finally, it examines physical security defenses that can be used to protect network technology devices.

Module 9, “Network Security Appliances and Technologies,” examines security appliances that provide resilience to attackers, such as firewalls, proxy servers, deception instruments, and other security appliances. It also explores security technologies such as access technologies, technologies for monitoring and managing and network, and principles for designing a secure network.

Module 10, “Cloud and Virtualization Security,” looks at both cloud computing and virtualization. It examines what both of these technologies are, how they function, and how they can be secured. Because cloud computing relies on secure network connections, it also discusses secure network protocols.

Module 11, “Wireless Network Security,” explores the attacks on wireless devices that are common today. It also identifies vulnerabilities in wireless security and examines several secure wireless protections.

Module 12, “Authentication,” defines authentication and the secure management techniques that enforce authentication. This module looks at the types of authentication credentials that can be used to verify a user’s identity and the techniques and technology used to manage user accounts in a secure fashion.

Module 13, “Incident Preparation, Response, and Investigation,” focuses on the plans that must be made for when a cybersecurity incident occurs. These plans cover incident preparation, incident response, and then a follow-up investigation as to how the incident occurred and how similar future events can be mitigated.

Module 14, “Cybersecurity Resilience,” explores the capacity of an organization to recover quickly from difficulties and spring back into shape. This module defines business continuity and why it is important. Next, it investigates how to prevent disruptions through redundancy. Finally, it explains how business policies can help provide resilience to an organization.

Module 15, “Risk Management and Data Privacy,” examines two elements of cybersecurity that are of high importance to both enterprises and users. The first involves risk and the strategies for mitigating risks. It also explores data privacy and the issues that surround it.

Healthy on the Hill

All students are strongly encouraged to [get the COVID-19 vaccine](#). Out of respect for the health and safety of the WKU community and in adherence with CDC guidelines and practices of all public universities and colleges in [Kentucky](#), the University requires that a cloth face covering (reusable or disposable) that covers both the nose and mouth must be worn at all times when in public areas within all buildings. Students must properly wear face coverings while in class regardless of the room size or the nature of the classroom activities. Students who fail to wear a face covering as required will be in violation of the WKU Student Code of Conduct and will be asked to comply or will face disciplinary action, including possible dismissal from the University. Accommodations can be requested in special cases through the Student Accessibility and Resource Center ([SARC](#)): [270-745-5004](#) (voice), [270-745-3030](#) (TTY), or [270-288-0597](#) (video).

All students must immediately report a positive Covid-19 test result or close contact with a person who has tested positive to the Covid-19 Assistance Line at 270-745-2019. The assistance line is available to answer questions regarding any Covid-19 related issue. This guidance is subject to change based on

requirements set forth by public health agencies or the office of the governor. Please refer to the Healthy on the Hill website for the most current information. www.wku.edu/healthyonthehill

ADA Accommodations

In compliance with University policy, students with disabilities who require academic and/or auxiliary accommodations for this course must contact the Student Accessibility Resource Center located in Downing Student Union, Room 1074. The SARC can be reached by phone number at 270-745-5004 [270-745-3030 TTY] or via email at sarc.connect@wku.edu. Please do not request accommodations directly from the professor or instructor without a faculty notification letter (FNL) from The Student Accessibility Resource Center.

If you have received an FNL you are required to meet with your instructor during scheduled office hours in order to discuss how the accommodations requested will be served in this course. Do NOT email your FNL to your instructor requesting a signature; rather, you must first meet with your instructor.

The Blackboard Ally tool has been enabled within the Blackboard course site that allows you to have access to different formats of course files, including HTML, readable PDF, electronic braille, ePub, and audio (mp3). You may review the [Ally for Students video](#) regarding how to access these alternative formats.

Additional Assistance

- *Research Appointments with your Personal Librarian* - At WKU Libraries, a personal librarian is available for every program on campus, plus Special Collection librarians and archivists. Our goal is to save you time and help you be successful on term papers and research projects by showing you what you need to know to get started and be successful. Start your research by scheduling an appointment with your Personal Librarian (you can find them listed online [here](#)) by emailing your Personal Librarian or calling (270)745-6125.
- *Writing Center Assistance* - The Writing Center on the Bowling Green campus is offering only remote assistance to writers during the COVID-19 pandemic. WKU students may request feedback on their writing via email or arrange a real-time Zoom conference to discuss a paper. See instructions and how-to videos on the website (www.wku.edu/writingcenter) for making online synchronous (Zoom) or asynchronous (email) appointments. Students may also get short writing questions answered via email; just put "Quick question" in the subject line to (writingcenter@wku.edu). The WKU Glasgow START Center/Writing Center will be offering writing tutoring sessions in synchronous online format as well as in person, by appointment only. More information on how to make appointments and what to expect from your appointment will continue to be posted at <https://www.wku.edu/startcenter/>.
- *WKU Counseling and Testing Center* - The university experience should be challenging, but not overwhelming. To this end, the WKU Counseling Center provides a variety of services to help strengthen students' capacity to tolerate distress, form healthy relationships, and seek healthy expressions of their ideals and values. If you would like to speak with someone, you may contact WKU's [Counseling and Testing Center](#) at 270-745-3159 or use their Here To Help service

at <https://www.wku.edu/heretohelp/heretohelpemail.php>. If you need immediate help, please visit the Counseling Center in 409 Potter Hall or call the 24-hour emergency help line at 270-843-4357.

- *Mental Health Support Group* - A Free Support/Recovery Group for current WKU students struggling with anxiety, depression, or other mental health issues is available. This is an opportunity for students to support, connect with, and encourage others struggling with mental health issues and is led by two National Alliance on Mental Illness (NAMI) certified facilitators who are in mental health recovery themselves. This group has the support of the WKU Counseling and Testing Center and is not a substitute (rather a supplement) for therapy or medication. No formal mental health diagnosis is required for students to attend. The group is sponsored by the NAMI-Bowling Green Chapter.
- *Peer Tutoring Services* - The Learning Center (TLC) provides free tutoring services that empower students to achieve academic success. Trained peer tutors are available to review course content, answer questions, and demonstrate effective study strategies. TLC offers individual appointments and group sessions (PASS) for hundreds of undergraduate courses. For more information or to make an appointment, visit www.wku.edu/tlc.

Title IX /Discrimination & Harassment

WKU is committed to supporting faculty, staff and students by upholding WKU's [Title IX Sexual Misconduct/Assault Policy \(#0.2070\)](#) and [Discrimination and Harassment Policy \(#0.2040\)](#). Western Kentucky University (WKU) is committed to supporting faculty, staff and students by upholding WKU's Title IX Sexual Misconduct/Assault Policy (#0.2070) and Discrimination and Harassment Policy (#0.2040). Under these policies, discrimination, harassment and/or sexual misconduct based on sex/gender are prohibited. If students experience an incident of sex/gender-based discrimination, harassment and/or sexual misconduct, they are encouraged to report it to the Title IX Coordinator (Andrea Anderson, 270-745-5398) or Title IX Investigators (Michael Crowe, 270-745-5429 or Joshua Hayes, 270-745-5121). Please note that while students may report an incident of sex/gender based discrimination, harassment and/or sexual misconduct to a faculty member, WKU faculty are considered "Responsible Employees" of the University and must report what is shared to WKU's Title IX Coordinator or Title IX Investigator. Students who would like to speak with someone who may be able to afford confidentiality may contact WKU's Counseling and Testing Center (270-745-3159).

Academic Dishonesty

"[Academic dishonesty] is a very serious academic offense. In a way, the very foundation of the American educational system rests on the issue of trust, and this trust depends on an honest exchange between students and their teachers. Just as students need to trust that teachers are honest about grading, teaching, and advising, teachers need to trust that students will be honest when taking tests and writing papers. Plagiarism, or any type of cheating, seriously undermines this foundation. This sort of dishonesty indicates that there may be serious questions about the offending student's ethics, and the stigma of this unethical behavior may follow the student for years—decreasing the student's chances of success in academic and professional work (adopted from Department of English Policy and Frequently Asked Questions on Plagiarism).

Students are expected to do work that is assigned to them and submit products that represent personal and individual effort **only**. This principle generally applies to all work done for a class, regardless of the nature of the assignment. When students breach this fundamental guideline, it can be safely assumed that academic dishonesty has occurred. Examples include:

1. In an exam setting
 - a. Presenting as your work test answers that are not your work, which includes i) Using resources other than those specifically allowed by the instructor (e.g., notes or another person); ii) Copying from another student's test; iii) Using notes from any source during a test when notes are not allowed; iv) Using materials that the instructor is not making available to the whole class; v) Recycling an assignment that has been used in another course
 - b. Acquiring a copy of the exam without permission
 - c. Providing answers for or soliciting answers from another student with or without permission of the other student
2. On a written assignment
 - a. Presenting as your own work duplicated work that you did not create by i) Purchasing written work from an external source; ii) Copying work from a free external source (online or otherwise); iii) Presenting as your work something another person has created
 - b. Altering text from another source or altering select words of some original text in order to conceal plagiarism
3. Other
 - a. Providing money or favors in order to gain academic advantage
 - b. Falsely stating that work was given to the instructor at a certain time when it was not
 - c. Correcting the responses of a graded assignment and presenting them to the instructor as incorrectly graded material
 - d. Pretending to be someone you are not; taking the place of another
 - e. Any other behavior that violates the basic principles of integrity and honesty

(Adopted from College of Education and Behavioral Sciences Academic Integrity Statement)

The WKU policy permits a faculty member to fail the student on the item on which academic dishonesty occurred or for the entire course. Cases of academic dishonesty will be handled as followed:

1. The student will receive a zero (0) for the assignment or an F for the course.
2. The incident will be reported to the CIS department chairperson.
3. The incident will be reported to the Dean of the College of Business.
4. The incident will be reported to the Office of Student Conduct. The student will be notified of the violation and a disciplinary conference will be scheduled. At this meeting the Director will complete in the presence of the student the following forms: Judicial Process form, Disciplinary Outcome Conference form, and Parental Notifications and Creative Discipline Referral forms. Once the student accepts responsibility for violating university policies the sanction process begins to change the student's behavior and create a commitment to living within the standards of the Code of Conduct. In addition notifications will be sent to the appropriate

stakeholders. A permanent reference to the incident may be placed on the student's permanent transcript.

5. Expulsion from the University may occur at the recommendation of the University Disciplinary Committee.