TRINE UNIVERSITY

# Course Syllabus

**Course Title:** Cybersecurity

**Term and Year:**

**Course and Section Number:** IS 5403

**Time and Place:**

**Number of Credit Hours:** 3

**Instructor:**

**Office Location/Hours:**

**Office Phone:**

**Email:**

**Course Description:** This course provides knowledge and practical skills required for a variety of cybersecurity roles. Throughout this course, students will use technologies and tools to identify and address security threats, attacks and vulnerabilities. Emphasis is placed on the latest trends and techniques in risk management, risk mitigation, threat management and intrusion detection. This course also covers principles and foundations of network architecture and design, cryptography, and PKI.

**Prerequisites:** IS 5203 Network Management

**Learning Outcomes:** Upon completion of this course, the student should be able to:

1. Compare elements of cybersecurity to societal vulnerabilities.
2. Assess threats, vulnerabilities, and intelligence to reduce exposure to attacks.
3. Evaluate cryptography by weighing its importance to data security.
4. Design simple computer networks and secure protocols for safe network usage.
5. Develop firewalls, intrusion detection, and intrusion protection approaches to ensure security of networks.
6. Implement secure network architecture practices.
7. Create organizational cybersecurity processes and procedures.

**Required Text:** None

**References:** Coursera: IBM Cybersecurity Analyst Professional Certificate (www.coursera.org)
IBM Cybersecurity Analyst Professional Certificate | Coursera

**Other Materials:**

**Course Requirements:** Coursera: IBM Cybersecurity Analyst Professional Certificate (www.coursera.org)

**Attendance/Participation:** All students are expected to log in to their courses regularly throughout the week to receive instruction, materials, and updates from the instructor. It is your responsibility to check in and submit your assignments, complete your discussion board postings, and finish quizzes and exams by the due dates.

If you do not participate in the course, you will be counted absent. Simply logging in is not enough; you must submit/complete an assignment, post to a discussion board, or other similar assignment tasks to avoid being counted absent. Instructors are required to submit attendance the Monday following each week of class.

This attendance is reported to the Financial Aid Department and may result in the loss of any financial aid refund you are expecting if you have not been participating in your courses. **In addition, you will be administratively dropped from the course if you are reported absent a total of three weeks.**

If this is a HYBRID class, please ensure that you arrive at 7am. Lateness is not tolerated. If you are going to miss the in-person class, notify your instructor AND academic advisor so you can fill out an extreme circumstances letter. Only EXTREME circumstances will be approved. Please make every effort to attend as scheduled.

**Grading/Evaluation:**

| Assignments | Amount | Value | Points | Percentage |
|---|---|---|---|---|
| Discussion Forum | 4 | 50 | 200 | 15% |
| Coursera Quizzes | 33 | 100 | 3300 | 23% |
| Podcast Quizzes | 4 | 100 | 400 | 15% |
| Storytime Video Responses | 6 | 50 | 300 | 10% |
| Reflection Blogs | 7 | 50 | 350 | 15% |
| Architecture Video Responses | 10 | 50 | 500 | 20% |
| Coursera IBM Capstone | 1 | 50 | 50 | 2% |
| Total | 141 | - | 5100 | 100% |

**Trine Graduate Grading Scale:**

| Grade | Percentage | Quality Points | Meaning of Grade |
|---|---|---|---|
| **A** | 93-100 | 4.0 | Excellent |
| **B+** | 86-92 | 3.5 | Very Good |
| **B** | 81-85 | 3.0 | Good |
| **C+** | 75-80 | 2.5 | Above Average |
| **C** | 70-74 | 2.0 | Average (lowest passing grade) |
| **F** | 00-69 | 0.0 | Failure |
| **I** | Incomplete | Not figured into GPA | |
| **IP** | In Progress (grade deferred) | Not figured into GPA | |
| **W** | Withdrawal | Withdrawal before completion of 80% of semester | |

| | | | |
|---|---|---|---|
| **WP** | Withdrawal | Withdrawal after completion of 80% of semester issued only under special circumstances and with approval of the department chair/director | |

**Other Policies:**

**Artificial Intelligence Policy:**
**Artificial Intelligence (AI) is prohibited:** All work submitted by students in this course must be generated by the student. Students may not have another person or entity contribute to an assignment for them, which includes using AI. Students may not incorporate any part of an AI-generated response in an assignment, use AI to formulate arguments, use AI to generate ideas for an assignment, or submit work to an AI platform for improvement. Using an AI tool to generate content may qualify as academic misconduct in this course.

OR

**Artificial Intelligence (AI) is allowed:** Students may use AI tools on instructor-identified assignments in this course. To adhere to our scholarly values, students must cite any AI-generated material that informed their work. Using an AI tool without proper attribution may qualify as academic misconduct in this course. It is the responsibility of the student to verify the accuracy, reliability, and ethical implications of AI-generated content.

**Academic Misconduct:**
The University prohibits all forms of academic misconduct. Academic misconduct refers to dishonesty in examinations (cheating), presenting the ideas or the writing of someone else as one's own (plagiarism) or knowingly furnishing false information to the University by forgery, alteration, or misuse of University documents, records, or identification. Academic dishonesty includes, but is not limited to, the following examples: permitting another student to plagiarize or cheat from one's own work, submitting an academic exercise (written work, printing, design, computer program) that has been prepared totally or in part by another, acquiring improper knowledge of the contents of an exam, using unauthorized material during an exam, submitting the same paper in two different courses without knowledge and consent of professors, or submitting a forged grade change slip or computer tampering. The faculty member has the authority to grant a failing grade in cases of academic misconduct as well as referring the case to Student Life.

**Plagiarism:**
You are expected to submit your own work and to identify any portion of work that has been borrowed from others in any form. An ignorant act of plagiarism on final versions and minor projects, such as attributing or citing inadequately, will be considered a failure to master an essential course skill and will result in an F for that assignment. A deliberate act of plagiarism, such as having someone else do your work, or submitting someone else's work as your own (e.g., from the Internet, fraternity file, etc., including homework and in-class exercises), will at least result in an F for that assignment and could result in an F for the course.

**Electronic Devices:**
Use of electronic devices including smart watches and cell phones is prohibited during exams or quizzes unless directly allowed by the instructor.

**Course Mapping:**

| Week and Title | Learning Activities and Materials (LO alignment) | Assessments (LO alignment) |
|---|---|---|
| **Week One:** Introduction to Cybersecurity Tools & Cyber Attacks | Listen & Read (Coursera):<br>1. History of Cybersecurity – 17 videos, 9 Readings (LO1)<br>2. Types of Actors and Their Motives – 27 videos, 3 Readings (LO2)<br>3. Overview of Key Security Concepts – 14 videos, 4 Readings (LOs 1,4,6,7)<br>4. Overview of Key Security Tools – 16 videos, 2 Readings (LOs 5-6)<br><br>Listen (Podcasts & Stories):<br>1. "Up in the Air" with Dr. Brandon McIver (Cyber Security Tools vs Cyber Defense Tools) 27:06 (LOs 4-7)<br>2. "Storytime" with Dr. Brandon McIver (Operational Cyber) 15:25 (LOs 4-7) | 1. History of Cybersecurity – 7 Quizzes (LO1)<br>2. Types of Actors and Their Motives – 7 Quizzes (LO2)<br>3. Overview of Key Security Concepts – 5 Quizzes (LO 1,4,6,7)<br>4. Overview of Key Security Tools – 5 Quizzes (LOs 5-7)<br>5. Podcast Discussion (LOs 4-7)<br>6. Podcast Quiz (LOs 4-7)<br>7. Storytime Video Response (LOs 4-7)<br>8. Week 1 Reflection Blog (LOs 4-7)<br>9. Certificate and Score Submissions (LOs 1-2, 4-7) |
| **Week Two:** Cybersecurity Roles, Processes, & Operating System Security | Listen & Read (Coursera):<br>1. People Process & Technology – 9 videos, 4 readings (LO7)<br>2. Examples & Principles of the CIA Triad – 5 videos, 1 reading (LO6) (LO7)<br>3. Authentication and Access Control – 5 videos, 1 reading (LO6) (LO7)<br>4. Windows OS Security Basics – 6 videos (LO6) | 1. People Process & Technology –4 Quizzes (LO7)<br>2. Examples & Principles of the CIA Triad – 2 quizzes (LO6) (LO7)<br>3. Authentication and Access Control – 3 quizzes (LO6) (LO7)<br>4. Windows OS Security Basics – 4 quizzes (LO6)<br>5. Linux OS Security Basics – 4 quizzes (LO6)<br>6. macOS Security Basics – 1 quiz (LO6)<br>7. Overview of Virtualization – 2 quizzes (LO6)<br>8. Podcast Discussion (LO6) (LO7)<br>9. Podcast Quiz (LO6) (LO7)<br>10. Storytime Video Response (LO6) (LO7)<br>11. Week 2 Reflection Blog (LO6) (LO7)<br>12. Certificate and Score Submissions (LO6) |

| | | |
|---|---|---|
| | 5. Linux OS Security Basics – 4 videos, 3 readings (LO6)<br><br>6. macOS Security Basics – 3 videos, 1 reading (LO6)<br><br>7. Overview of Virtualization – 6 videos, 1 reading (LO6)<br><br>Listen (Podcasts & Stories):<br>1. "Up in the Air" with Dr. Brandon McIver (Cybersecurity Leadership and Operations) 33:48 (LO1) (LO2)<br><br>2. "Storytime" with Dr. Brandon McIver (The Cybersecurity Spectrum) 11:20 (LO6) (LO7) | (LO7) |
| **Week Three:** Cybersecurity Compliance Framework & System Administration | Listen & Read (Coursera):<br>1. Compliance Frameworks and Industry Standards – 13 videos, 8 readings (LO4)<br><br>2. Client System Administration, Endpoint Protection and Patching – 7 videos, 5 readings (LO4) (LO5)<br><br>3. Server and User Administration – 21 videos, 3 readings (LO4) (LO5)<br><br>4. Cryptography and Compliance Pitfalls – 12 videos, 8 readings (LO3)<br><br>5. Linux and Encryption: Final Project – 1 video, 1 reading (LO3) (LO4)<br><br>Listen (Podcasts & Stories):<br>1. "Storytime" with Dr. Brandon McIver (Why Frameworks Matter) 13:29 (LO1) (LO2)<br><br>Watch:<br>1. Cybersecurity Architecture Principles 17:34 (LO6) (LO7)<br><br>2. Cybersecurity Architecture Fundamentals 12:34 (LO6) (LO7) | 1. Compliance Frameworks and Industry Standards – 5 quizzes (LO4)<br>2. Client System Administration, Endpoints Protection and Patching – 3 quizzes (LO4) (LO5)<br>3. Server and User Administration – 3 quizzes (LO4) (LO5)<br>4. Cryptography and Compliance Pitfalls – 3 quizzes (LO3)<br>5. Storytime Video Response (LO2)<br>6. Cybersecurity Architecture: Principles Response (Presentation) 2:00 (LO6) (LO7)<br>7. Cybersecurity Architecture: Fundamentals Response (Presentation) 2:00 (LO6) (LO7)<br>8. Week 3 Reflection Blog (LO2)<br>9. Certificate and Score Submissions (LOs 3-5) |

| | | |
|---|---|---|
| **Week Four:** Network Security & Database Vulnerabilities | Listen & Read (Coursera):<br>1. TCP/IP Framework – 16 videos, 3 readings (LO4)<br><br>2. Basics of IP Addressing and the OSI Model – 16 videos (LO4)<br><br>3. Introduction to Databases – 18 videos, 1 reading (LO4)<br><br>4. Deep Dive – Injection Vulnerability – 8 videos, 5 readings (LO6)<br><br>5. Final Project (LO4) (LO6)<br><br>Listen (Podcasts & Stories):<br>1. "Up in the Air" with Dr. Brandon McIver (Let's talk Databases and Developers) 32.24 (LO6)<br><br>2. "Storytime" with Dr. Brandon McIver (Vulnerability Management) 10:33 (LO4) (LO6) | 1. TCP/IP Framework – 4 quizzes (LO4)<br>2. Basics of IP Addressing and the OSI Model – 6 quizzes (LO4)<br>3. Introduction to Databases – 4 quizzes (LO4)<br>4. Deep Dive – Injection Vulnerability – 4 quizzes (LO6)<br>5. Final Project (LO4) (LO6)<br>6. Podcast Discussion (LO6)<br>7. Podcast Quiz (LO6)<br>8. Storytime Video Response (LO4) (LO6)<br>9. Week 4 Reflection Blog (LO4) (LO6)<br>10. Certificate and Score Submissions (LO4) (LO6) |
| **Week Five:** Penetration Testing, Incident Response and Forensics | Listen & Read (Coursera):<br>1. Penetration Testing – 8 videos, 7 readings (LO2)<br><br>2. Incident Response – 9 videos, 8 readings (LO7)<br><br>3. Digital Forensics – 8 videos, 3 readings (LO2)<br><br>4. Introduction to Scripting – 9 videos, 7 readings (LO6)<br><br>Listen (Podcasts & Stories):<br>1. "Storytime" with Dr. Brandon McIver (Stop the Madness of Incident Response) 15:03 (LO6) (LO7)<br><br>Watch:<br>1. Cybersecurity Architecture: Detection 17:10 (LO6) (LO7)<br><br>2. Cybersecurity Architecture: Response 16:57 (LO6) (LO7) | 1. Penetrating Testing – 4 quizzes (LO2)<br>2. Incident Response – 2 quizzes (LO7)<br>3. Digital Forensics – 4 quizzes (LO2)<br>4. Introduction to Scripting – 3 quizzes (LO6)<br>5. Storytime Video Response (LO6) (LO7)<br>6. Cybersecurity Architecture: Detection - Response (Presentation) 2:00 (LO6) (LO7)<br>7. Cybersecurity Architecture: Response - Response (Presentation) 2:00 (LO6) (LO7)<br>8. Week 5 Reflection Blog (LO2) (LO6) (LO7)<br>9. Certificate and Score Submissions (LO2) (LO6) (LO7) |
| **Week Six:** | Listen & Read (Coursera): | 1. Threat Intelligence – 3 quizzes (LO1) (LO2) |

| | | |
|---|---|---|
| Cyber Threat Intelligence | 1. Threat Intelligence – 5 videos, 3 reading (LO1) (LO2)<br><br>2. Data Loss Prevention and Mobile Endpoint Protection – 8 videos, 2 readings (LO2)<br><br>3. Scanning – 3 videos, 1 reading (LO5)<br><br>4. Application Security and Testing – 12 videos, 1 reading (LO5)<br><br>5. SIEM Platforms – 7 videos, 4 readings (LO5)<br><br>6. Threat Hunting – 3 videos, 3 readings (LO2) (LO5)<br><br>Listen (Podcasts & Stories):<br>1. "Up in the Air" with Dr. Brandon McIver (Cyber Threat Intelligence) 33:37 (LO1)<br><br>2. "Storytime" with Dr. Brandon McIver (Contested Environment) 13:39 (LO1) (LO2) | 2. Data Loss Prevention and Mobile Endpoint Management – 3 quizzes (LO2)<br>3. Scanning – 4 quizzes (LO5)<br>4. Application Security and Testing – 5 quizzes (LO5)<br>5. SIEM Platforms – 3 quizzes (LO5)<br>6. Threat Hunting – 2 quizzes (LO2) (LO5)<br>7. Podcast Discussion (LO1)<br>8. Podcast Quiz (LO1)<br>9. Storytime Video Response (LO1) (LO2)<br>10. Week 6 Reflection Blog (LO1) (LO2) (LO5)<br>11. Certificate and Score Submissions (LO1) (LO2) (LO5) |
| **Week Seven:** Cybersecurity Capstone: Breach Response Case Studies | Watch:<br>1. Cybersecurity Architecture Role & Tools 14:07 (LO6) (LO7)<br><br>2. Identity and Access Management 31:15 (LO6) (LO7)<br><br>3. Endpoint Management 14:22 (LO6) (LO7) | 1. Cybersecurity Capstone – Breach Response Case Studies (LO6) (LO7)<br>2. Cybersecurity Architecture Role & Tools Response (Presentation) 2:00 (LO6) (LO7)<br>3. Identity and Access Management Response (Presentation) 2:00 (LO6) (LO7)<br>4. Endpoint Management Response (Presentation) 2:00 (LO6) (LO7)<br>5. Week 7 Reflection Blog (LO1)(LO2)(LO6) (LO7) |
| **Week Eight:** IBM Cybersecurity Architecture | Watch:<br>6. Cybersecurity Architecture Network Security 27:31 (LO6) (LO7)<br><br>7. Cybersecurity Architecture: Application Security 16:36 | 3. Cybersecurity Architecture Role & Tools Response (Presentation) 2:00 (LO6) (LO7)<br>4. Identity and Access Management Response (Presentation) 2:00 (LO6) (LO7)<br>5. Endpoint Management Response (Presentation) 2:00 (LO6) (LO7)<br>6. Cybersecurity Architecture Network Security |

| | | |
|---|---|---|
| | (LO6) (LO7)<br><br>8. Cybersecurity Architecture: Data Security 14:48 (LO6) (LO7) | Response (Presentation) 2:00 (LO6) (LO7)<br>7. Cybersecurity Architecture: Application Security Response (Presentation) 2:00 (LO6) (LO7)<br>8. Cybersecurity Architecture: Data Security Response (Presentation) 2:00 (LO6) (LO7) |