CYBERSECURITY

BTU | BUSINESS & TECHNOLOGY UNIVERSITY

AI SYLLABUS

Cybersecurity

Course Description:

This course introduces students to the fundamentals of cybersecurity, with a focus on cybersecurity strategy, risk management, incident response, and digital forensics. Through a combination of lectures, case studies, and hands-on exercises, students will learn about the current threat landscape, the importance of cybersecurity in today's world, and the techniques and tools used to protect against cyberattacks.

Course Goals:

- Understand the importance of cybersecurity and the current threat landscape.
- Develop the knowledge and skills to develop a cybersecurity strategy and risk management plan.
- Learn how to respond to cyber incidents and conduct digital forensics investigations.
- Develop critical thinking skills that allow students to evaluate cybersecurity issues and make informed decisions in a variety of contexts.

Course Outline:

Week 1: Introduction to Cybersecurity

1. Overview of cybersecurity and the current threat landscape
2. Cybersecurity frameworks and standards
3. Risk management in cybersecurity

Week 2: Cybersecurity Strategy and Planning

1. Developing a cybersecurity strategy
2. Implementing a cybersecurity risk management plan
3. Best practices in cybersecurity planning

Week 3: Incident Response and Recovery

1. Responding to a cybersecurity incident
2. Incident response planning and preparation
3. Business continuity and disaster recovery planning

Week 4: Digital Forensics and Investigations

1. Introduction to digital forensics
2. Conducting a digital forensics investigation
3. Best practices in digital forensics

Assessment and Evaluation:

- Participation and Attendance: 10%
- Homework Assignments: 30%
- Midterm Exam: 20%
- Final Exam: 40%

Required Readings:

1. Cybersecurity and Cyberwar: What Everyone Needs to Know by P.W. Singer and Allan Friedman
2. Data Breach: Preparation and Response by Kevvie Fowler and George Hulme
3. Principles of Incident Response and Disaster Recovery by Michael E. Whitman and Herbert J. Mattord
4. Cybersecurity: The Beginner's Guide by Raef Meeuwisse
5. Incident Response & Computer Forensics by Jason Luttgens, Matthew Pepe, and Kevin Mandia
6. The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes by Dawn M. Cappelli, Andrew P. Moore, and Randall F. Trzeciak

Course Assignments:

- Develop a cybersecurity strategy and risk management plan for a small business.
- Conduct a tabletop exercise to simulate a cybersecurity incident and develop an incident response plan.
- Conduct a digital forensics investigation on a simulated cybercrime scenario.

Classroom Policies:

- Attendance and participation are expected in every class. If you have to miss a class, please notify the instructor in advance.

- Late homework assignments will not be accepted without prior approval from the instructor. If you have an emergency or an unexpected situation that prevents you from completing an assignment on time, please contact the instructor as soon as possible.
- Academic dishonesty, including plagiarism and cheating, will not be tolerated and will result in a failing grade for the course. It is the responsibility of each student to ensure that their work is original and properly cited.
- Students are expected to treat each other and the instructor with respect and professionalism. Inappropriate behavior, including harassment and discrimination, will not be tolerated and may result in disciplinary action.
- Accommodations for students with disabilities are available through the Disability Services Office. If you require accommodations, please contact the instructor and the Disability Services Office as soon as possible to make arrangements.

Course Resources:

- Virtual machines with pre-configured cybersecurity tools will be provided to students.
- Virtual labs and exercises: Students can practice cybersecurity skills in a virtual environment using pre-configured virtual machines and exercises. These resources can help students gain hands-on experience in threat identification, risk management, and incident response.
- Cybersecurity communities: Online communities and forums can provide students with opportunities to connect with professionals in the cybersecurity field, ask questions, and share knowledge.
- Cybersecurity conferences: Attending cybersecurity conferences can provide students with opportunities to learn about the latest trends and best practices in cybersecurity, network with professionals in the field, and gain insights into potential career paths.
- Cybersecurity certifications: Students may choose to pursue cybersecurity certifications, such as CompTIA Security+, Certified Information Systems Security Professional (CISSP), or Certified Ethical Hacker (CEH), to gain additional knowledge and credentials in the field.
- Cybersecurity podcasts and webinars: Listening to cybersecurity podcasts or attending cybersecurity webinars can provide students with additional insights into the field, including current threats, new technologies, and emerging trends.