STATE UNIVERSITY OF NEW YORK
COLLEGE OF TECHNOLOGY
CANTON, NEW YORK

MASTER SYLLABUS

CYBR 416– Cybersecurity in Healthcare

Created by: Rich Ingersoll
Updated by:

SCHOOL OF SCIENCE, HEALTH AND CRIMINAL JUSTICE
CENTER FOR CRIMINAL JUSTICE, INTELLIGENCE AND CYBERSECURITY
SPRING 2023

A. **TITLE**: Cybersecurity in Healthcare

B. **COURSE NUMBER:** CYBR 416

C. **CREDIT HOURS:** 3

D. **WRITING INTENSIVE COURSE**: No

E. **GER CATEGORY:** None

F. **SEMESTER(S) OFFERED:** Fall and Spring

G. **COURSE DESCRIPTION:** This course provides a high-level overview of the current state of Cybersecurity in the HealthCare Industry. Students will examine current threats and trends, provide insight as to why Healthcare is such a target rich environment, and discuss ways to mitigate these risks while still allowing Healthcare staff the ability to do their jobs successfully.

H. **PRE-REQUISITES/CO-REQUISITES:**

Prerequisite: 45 completed credit hours or permission of instructor.
Co-requisite: None
Pre- or co-requisite(s): None

I. **STUDENT LEARNING OUTCOMES:**

Course Student Learning Outcome [SLO]	***Program Student Learning Outcome [PSLO]***	***ISLO***
Examine Cybersecurity threats to Healthcare Systems and why Healthcare is a consistently growing target.	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	2[IA]
Determine mitigation techniques for vulnerabilities and attacks.	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	2[CA]

Evaluate the different phases of the attack process and how an attacker can penetrate a company.	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	2[IA]
Explain different types of attacks that are used on Hospitals or Healthcare Facilities.	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	2[IA]

KEY	**Institutional Student Learning Outcomes [ISLO 1 – 5]**
ISLO #	**ISLO & Subsets**
1	**Communication Skills** Oral [O], Written [W]
2	**Critical Thinking** *Critical Analysis [CA] , Inquiry & Analysis [IA] , Problem Solving [PS]*
3	**Foundational Skills** *Information Management [IM], Quantitative Lit,/Reasoning [QTR]*
4	**Social Responsibility** *Ethical Reasoning [ER], Global Learning [GL], Intercultural Knowledge [IK], Teamwork [T]*
5	**Industry, Professional, Discipline Specific Knowledge and Skills**

J. APPLIED LEARNING COMPONENT: **Yes _** **No _X_**

K. TEXTS:

Ayala, Luis (2016). *Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention*. APress.

L. REFERENCES:

Various internet sources (YouTube, CISA, others)

M. EQUIPMENT: None

N. GRADING METHOD: A-F

O. SUGGESTED MEASUREMENT CRITERIA/METHODS:

- Quizzes
- Exams

- Discussion Boards
- Case studies

P. <u>DETAILED COURSE OUTLINE</u>:

I. What is the Threat/Problem
II. The Attacker Process
III. Gaining Access
IV. Medical Device and Facility Specific Attacks
V. The Insider Threat
VI. Attack Detection
VII. Attack Prevention and Planning
VIII. Attack Response and Recovery

Q. <u>LAB</u> NA