School of Computing and Information Sciences

Course Title: Enterprise Cybersecurity Policies and Practices **Date:** 1/18/2018

Course Number: CIS 4365

Number of Credits: 3

Subject Area: Security	**Subject Area Coordinator:** **email:**
Catalog Description: Policies and practices for information assurance, incident response, disaster recovery, cost assessment, vulnerability assessment, vulnerability testing.	
Textbook: Security Policies and Implementation Issues, Second Edition. Robert Johnson. 2015. 9781284055993 Jones & Bartlett	
Prerequisites Courses: CNT 4403 or EEL 4806	
Corequisites Courses: None	

Type: Elective in cybersecurity concentration for IT

Prerequisite Topics:

- Fundamental concepts of Operating Systems
- Strong networking concepts, especially TCP/IP
- Basic security concepts

Course Outcomes:

1. Describe major developments in models of security services and countermeasures.
2. Prepare a threat analysis and appropriate countermeasures.
3. Identify risks associated with various types of company assets and quantitative and qualitative metrics for evaluating risks and countermeasures.
4. Perform a comprehensive risk assessment for a specified organization.
5. Justify appropriate mitigation strategies by comparing the costs associated with a specific risk and the mitigation strategy.
6. Describe the purpose and elements of the key types of security audits. Discuss how various security standards (i.e. ISO 177799) impact the direction of these audits.
7. Describe legal and ethical considerations related to the handling and management of enterprise information assets.
8. Develop an incident handling report

9. Create a business impact analysis (BIA) including cost/risk comparisons
10. Discuss the role of CASPR (Commonly Accepted Security Practices and Recommendations) forms in defining and approving standard operational and management practices.
11. Be able to identify how vulnerability in one area of an organization might enable a compromise in another area.

School of Computing and Information Sciences

CIS 4365 Enterprise Cybersecurity Policies and Procedures

Outline

Topic	Number of Lecture Hours	Outcome
Models of security services and countermeasures	3	1
Threat analysis and appropriate countermeasures	7	2, 3, 4
Risk analysis using quantitative and qualitative metrics for evaluating risks and countermeasures	5	2, 3, 4
Mitigation strategies	3	5
Security audits (based on standards such as ISO 27000)	5	6, 10
Legal and ethical considerations related to the handling and management of enterprise information assets	5	7
Incident handling report	5	8, 10
Business Impact Analysis and Disaster Recovery	7	9, 10, 11

School of Computing and Information Sciences

CIS 4365 Enterprise Cybersecurity Policies and Procedures

Course Outcomes Emphasized in Laboratory Projects / Assignments

Outcome	Number of Weeks
Risk Analysis including BIA	3
Mitigation Strategies including DR	5
Incident Report	2
Threat Analysis	2

Oral and Written Communication: BIA, DR, IR

Number of written reports: 3
Approximate number of pages for each report: 5-7
Number of required oral presentations: 1
Approximate time for each presentation: 10 minutes

Social and Ethical Implications of Computing Topics

Describe legal and ethical considerations related to the handling and management of enterprise information assets. (7)

Theoretical Contents

Topic	Class Time
IAS Fundamentals (Models of IAS and Threat Assessment)	6 hrs
IAS Operations (IR, DR, Ethical Considerations)	15 hrs
IAS Risk Assessment & Mitigation	15 hrs
IAS Policy	6 hrs

Problem Analysis Experiences

N/A

Solution Design Experiences

N/A

The Coverage of Knowledge Units within Computer Science Body of Knowledge[1]

Knowledge Unit	Topic	Type	Lecture Hours
IAS Fundamentals	Models of security services and countermeasures	Tier 1	3
IAS Threat Analysis	Threat analysis and appropriate countermeasures	Tier 1	7
IAS Threat Analysis	Risk analysis using quantitative and qualitative metrics for evaluating risks and countermeasures	Tier 1	5
IAS Operations	Mitigation strategies	Tier 1	3
IAS Operations	Security audits (based on standards such as ISO 27000)	Tier 1	5
IAS Operations	Legal and ethical considerations related to the handling and management of enterprise information assets	Tier 1	5
IAS Operations	Incident handling report	Tier 2	5
IAS Operations	Business Impact Analysis and Disaster Recovery	Tier 2	7
Total Hours			

[1]See http://www.acm.org/education/CS2013-final-report.pdf for a description of Computer Science Knowledge units