

Note:

Course content may be changed, term to term, without notice. The information below is provided as a guide for course selection and is not binding in any form, and should not be used to purchase course materials.

COURSE SYLLABUS

CSIS 343

CYBER-SECURITY

COURSE DESCRIPTION

A comprehensive overview of the essential concepts students must know as they pursue careers in information systems security. Topics include a discussion of the new risks, threats, and vulnerabilities associated with the transformation to a digital world, including a look at how business, government, and individuals operate today. Additionally, information is included from the Official (ISC) 2 SSCP Certified Body of Knowledge and presents a high-level overview of each of the seven domains within the System Security Certified Practitioner certification. (Formerly BMIS 342)

RATIONALE

Cyber security initiatives require a proactive and well-planned approach for defense measures. Such activities have to be thorough with respect to protections and exhaustive in regard to tracking and monitoring criminal activity. BMIS 343 looks at utilizing industry leading procedures for protecting, preventing, and tracking cyber-attacks.

I. PREREQUISITE

For information regarding prerequisites for this course, please refer to the [Academic Course Catalog](#).

II. REQUIRED RESOURCE PURCHASE

Click on the following link to view the required resource(s) for the term in which you are registered: <http://bookstore.mbsdirect.net/liberty.htm>

I. ADDITIONAL MATERIALS FOR LEARNING

- A. Computer with basic audio/video output equipment
- B. Internet access (broadband recommended)
- C. Microsoft Office

II. MEASURABLE LEARNING OUTCOMES

Upon successful completion of this course, the student will be able to:

- A. Discuss the relevance of course material and the use of technology to a biblical worldview.
- B. Recognize the appropriate steps for information security risk, response, and recovery.
- C. Annotate the basic concepts of cryptography to manage a secure infrastructure.

- D. Demonstrate the ability to assess and implement access controls.
- E. Explain how to identify and institute counter measures for malicious code.
- F. Analyze security issues, related networks, and systems.

III. COURSE REQUIREMENTS AND ASSIGNMENTS

- A. Readings and lecture presentations
- B. Course Requirements Checklist
After reading the Syllabus and [Student Expectations](#), the student will complete the related checklist found in Module/Week 1.
- C. Discussion Board Forums (8)
Discussion boards are collaborative learning experiences. Therefore, the student will participate in eight Discussion Board Forums. Threads must be at least 300 words integrating two biblical principles. In addition to the thread, the student must reply to at least two other classmates’ threads. Each reply must be at least 150 words.
- D. Exams (4)
The student will participate in four exams, each dealing with a different aspect of cyber security.
- E. Labs (8)
The student will submit eight labs, each dealing with a different aspect of cyber security.

IV. COURSE GRADING AND POLICIES

- A. Points

Course Requirements Checklist	10
Discussion Board Forums (8 at 35 pts ea)	280
Exams (4 at 80 pts ea)	320
Labs (8 at 50 pts ea)	400
Total	1010
- B. Scale
A = 900–1010 B = 800–899 C = 700–799 D = 600–699 F = 0–599
- C. Disability Assistance
Students with a documented disability may contact LU Online’s Office of Disability Academic Support (ODAS) at LUOODAS@liberty.edu to make arrangements for academic accommodations. Further information can be found at www.liberty.edu/disabilitysupport

COURSE SCHEDULE

CSIS 343

Textbook:
 Cengage Learning(2016). *Ethical Hacking and countermeasures* (2nd edition).

MODULE/ WEEK	READING & STUDY	ASSIGNMENTS	POINTS
1	Mindtap Module 1 <i>Attack phases</i>	Course Requirements Checklist	10
		DB Forum 1	35
		Module 1 Mindtap Lab	50
2	Mindtap Module 2 <i>Attack phases</i>	DB Forum 2	35
		Module 2 Mindtap Exam	80
		Module 2 Mindtap Lab	50
3	Mindtap Module 3 <i>Securing network operating systems and infrastructures</i>	DB Forum 3	35
		Module 3 Mindtap Lab	50
4	Mindtap Module 4 <i>Securing network operating systems and infrastructures</i>	DB Forum 4	35
		Module 4 Mindtap Exam	80
		Module 4 Mindtap Lab	50
5	Mindtap Module 5 <i>Threats and defense mechanisms</i>	DB Forum 5	35
		Module 5 Mindtap Lab	50
6	Mindtap Module 6 <i>Threats and defense mechanisms</i>	DB Forum 6	35
		Module 6 Mindtap Exam	80
		Module 6 Mindtap Lab	50
7	Mindtap Module 7 <i>Web applications and data servers</i>	DB Forum 7	35
		Module 7 Mindtap Lab	35
8	Mindtap Module 8 <i>Web applications and data servers</i>	DB Forum 8	35
		Module 8 Mindtap Exam	80
		Module 8 Mindtap Lab	50
TOTAL			1010

DB = Discussion Board

NOTE: Each course module/week (except Module/Week 1) begins on Tuesday morning at 12:00 a.m. (ET) and ends on Monday night at 11:59 p.m. (ET). The final module/week ends at 11:59 p.m. (ET) on **Friday**.