



Undergraduate Course Syllabus

CYB 320: Incident Response and Investigation

Center: Online

Course Prerequisites

CYB 300 and CYB 310

Course Description

Explore incident analysis and response techniques within the context of an enterprise. Learn basic digital forensic terminology and how incident response activities inform and augment digital investigations.

Course Outcomes

- Describe fundamentals of digital investigations
- Manage and resolve a cybersecurity incident
- Design business continuity and disaster recovery strategies based on organizational requirements

Required Materials

Using your learning resources is critical to your success in this course. Your textbook is available for free through the Shapiro Library.

[Business Continuity and Disaster Recovery Planning for IT Professionals](#)

Susan Snedaker

Syngress

Second Edition

September 2013

[CompTIA Server+ Certification Guide](#)

Ron Price

Packt Publishing

February 2019

[Investigating the Cyber Breach: The Digital Forensics Guide for the Network Engineer](#)

Aamir Lakhani and Joseph Muniz

Cisco Press

February 2018

[CHFI Computer Hacking Forensic Investigator Certification All-in-One Exam Guide](#)

Charles L. Brooks

McGraw-Hill Osborne Media

October 2014

[Hands-On Incident Response and Digital Forensics](#)

Mike Sheward

BCS Learning & Development Limited

July 2018

[The Basics of Digital Forensics](#)

John Sammons

Syngress

Second Edition

December 2014

Diversity, Equity, and Inclusion

As indicated in our core values, SNHU is committed to “embrace diversity where we encourage and respect diverse identities, ideas, and perspectives by honoring difference, amplifying belonging, engaging civilly, and breaking down barriers to bring our mission to life.”

This may or will be reflected in SNHU’s curriculum as we embrace and practice diversity, equity, and inclusion (DEI) to provide the most transformative experience for our students, faculty, and staff. Because topics pertaining to DEI can be sensitive, please remember that embodying and practicing diversity, equity, and inclusion is one of our core values that you will encounter throughout the academic experience. In higher education, we are expected to think and engage critically. Use a growth mindset to embrace the diverse readings, course assignments, and experiences of your peers and faculty.

For more information about DEI at SNHU, please visit our website at the [Office of Diversity and Inclusion](#).

Instructor Availability and Response Time

Your class interaction with the instructor and your classmates will take place on a regular, ongoing basis. Your instructor will be actively engaged within the course throughout the week. You will normally communicate with your instructor in the weekly discussions or the General Questions discussion topic so that your questions and the instructor’s answers benefit the entire class. You should feel free, however, to communicate with your instructor via SNHU email at any time, particularly when you want to discuss something of a personal or sensitive nature. Your instructor will generally provide a response within 24 hours. Instructors will post grades and feedback (as applicable) within seven days of an assignment’s due date, or within seven days of a late submission.

Grade Distribution

Assignment Category	Number of Graded Items	Point Value per Item	Total Points
Reading Quizzes	5	20	100
Discussions	4	25	100
Activities	2	50	100
Stepping Stones	4	70	280
SWOT Analysis	1	20	20
Playbook Submission	1	25	25
Competency Projects			
Project One	1	250	250
Project Two	1	125	125
			Total Course Points: 1,000

This course may also contain practice activities. The purpose of these non-graded activities is to assist you in mastering the learning outcomes in the graded activity items listed above.

University Grading System: Undergraduate

Grade	Numerical Equivalent	Points
A	93–100	4
A-	90–92	3.67
B+	87–89	3.33
B	83–86	3
B-	80–82	2.67
C+	77–79	2.33
C	73–76	2
C-	70–72	1.67
D+	67–69	1.33
D	60–66	1
F	0–59	0
I	Incomplete	
IF	Incomplete/Failure *	
IP	In Progress (past end of term)	
W	Withdrawn	

* Please refer to the [policy page](#) for information on the incomplete grade process.

Grading Guides

Specific activity directions, grading guides, posting requirements, and additional deadlines can be found in the Assignment Guidelines and Rubrics section of the course.

Weekly Assignment Schedule

All reading and assignment information can be found within each module of the course. Assignments and discussion posts during the first week of each term are due by 11:59 p.m. Eastern Time. Assignments and discussion posts for the remainder of the term are due by 11:59 p.m. of the student's local time zone.

In addition to the textbook readings that are listed, there may be additional required resources within each module.

Module	Topics and Assignments
1	Introduction to Incident Response and Investigation <i>Business Continuity and Disaster Recovery Planning for IT Professionals</i> , Chapter 1 <i>CompTIA Server+ Certification Guide</i> , Disaster Recovery chapter (up to and including Recovery Sites) 1-0 Knowledge Check (Non-graded) 1-1 Discussion: Introduction and Disaster Recovery 1-2 Reading Quiz 1-3 Review: Projects
2	Digital Forensics and Legal Dimensions <i>Investigating the Cyber Breach: The Digital Forensics Guide for the Network Engineer</i> , Chapter 4 <i>CHFI Computer Hacking Forensic Investigator Certification All-in-One Exam Guide</i> , Chapter 2 <i>Business Continuity and Disaster Recovery Planning for IT Professionals</i> , Chapter 2 2-0 Knowledge Check (Non-graded) 2-1 Reading Quiz 2-2 Activity: Forensic Law Worksheet 2-3 Project One Stepping Stone One: Incident Response Scenarios
3	The Incident Response Process <i>Hands-On Incident Response and Digital Forensics</i> , Chapters 3 and 4 3-0 Knowledge Check (Non-graded) 3-1 Reading Quiz 3-2 Activity: Incident Report Components 3-3 Project One Stepping Stone Two: Business Continuity Scenarios
4	Cybersecurity Architecture and SWOT Analysis 4-0 Knowledge Check (Non-graded) 4-1 Reading Quiz 4-2 SWOT Analysis: Personal Security and Home Technology 4-3 Project One Stepping Stone Three: Disaster Recovery Scenarios
5	Anti-Forensics and the Adversarial Mindset <i>The Basics of Digital Forensics</i> , Chapter 6 5-0 Knowledge Check (Non-graded) 5-1 Discussion: Anti-Forensic Methods and Adversarial Mindset 5-2 Reading Quiz 5-3 Project Two Stepping Stone: Digital Forensic Investigation Exploration
6	Incident Response and Recovery 6-1 Project One Submission: Incident Response and Recovery Recommendations

Module	Topics and Assignments
7	Digital Investigations and Legal Obligations 7-1 Discussion: Jurisdiction Issues 7-2 Project Two Submission: Digital Discovery Summary
8	Risk Management 8-1 Discussion: Risk Management 8-2 Cyber Playbook Submission

Course Participation

Course participation is required within the first week of the term for all online courses. *Participation* in this context is defined as completing one graded assignment during the first week of the course. Otherwise, students will be administratively removed for nonparticipation. Students who do not participate during the first week may forfeit their rights to be reinstated into the course. Students who stop attending a course after the first week and who do not officially withdraw will receive a grade calculated based on all submitted and missed graded assignments for the course. Missed assignments will earn a grade of zero. See the [course withdrawal policy](#) and the [full attendance policy](#) for further information.

Late Assignments

Students who need extra time may submit assignments (excluding discussion board postings) up to one week after the assignment due date. Discussion board submissions will not be accepted for credit after the deadline except in extenuating circumstances.

- A penalty of 10 percent of the total value of the assignment will be applied to the grade achieved on the late assignment regardless of the day of the week on which the work is submitted.
- Students who submit assignments more than one week late will receive a grade of zero on the assignment unless they have made prior arrangements with the instructor.

Students must submit all assignments no later than 11:59 p.m. (in their own time zone) on the last day of the term. No assignments are accepted after the last day of the term unless an incomplete has been submitted. See the [incomplete grades policy](#).

There may be times an instructor makes an exception to the late assignment policy. Instructors may accept late work, including discussion board posts, with or without prior arrangement.

- Exceptions to the late policy on these grounds are left to the instructor's discretion, including whether the late penalty is applied or waived. Students should not assume that they will be allowed to submit assignments after the due dates.
- If an instructor finds that they are unable to determine whether an exception to the late policy would be appropriate without documentation, the collection and review of student documentation should be handled through the Dispute Resolution team in order to protect the student's privacy. In these cases, students should file a [Student Concern Dispute form](#) to have the circumstances reviewed.

If a student is experiencing (or knows they will experience) a circumstance, including pregnancy, that is protected under the Americans with Disabilities Act or Title IX, they are encouraged to contact the [Online Accessibility Center](#)

[\(OAC\)](#) as soon as possible to explore what academic accommodations might be offered. Instructors must honor all deadlines established through the OAC.

Student Handbook

Review the [student handbook](#).

ADA/504 Compliance Statement

Southern New Hampshire University (SNHU) is dedicated to providing equal access to individuals with disabilities in accordance with Section 504 of the Rehabilitation Act of 1973 and with Title III of the Americans with Disabilities Act (ADA) of 1990, as amended by the Americans with Disabilities Act Amendments Act (ADAAA) of 2008.

SNHU prohibits unlawful discrimination on the basis of disability and takes action to prevent such discrimination by providing reasonable accommodations to eligible individuals with disabilities. The university has adopted the [ADA/504 Grievances Policy](#) (version 1.2 effective October 16, 2017), providing for prompt and equitable resolution of complaints regarding any action prohibited by Section 504 or the ADA.

For further information on accessibility support and services, visit the [Disability and Accessibility Services](#) webpage.

Academic Integrity Policy

Southern New Hampshire University requires all students to adhere to high standards of integrity in their academic work. Activities such as plagiarism and cheating are not condoned by the university. Review the [full academic integrity policy](#).

Copyright Policy

Southern New Hampshire University abides by the provisions of United States Copyright Act (Title 17 of the United States Code). Any person who infringes the copyright law is liable. Review the [full copyright policy](#).

Withdrawal Policy

Review the [full withdrawal policy](#).

Southern New Hampshire University Policies

More information about SNHU policies can be found on the [policy page](#).