BADM 7501:
Cybersecurity Risk Management

Table of Contents

Instructor & Course Information

BADM 7501: Cybersecurity Risk Management (3 credit hours)

Instructor: Wes Ladd, MBA

Please email your instructor or post in the Q&A forum with questions about course content. Every effort will be made to respond within 24 hours.

Catalog description: COMING FALL 2023

Pre/co-requisites: none

Program Outcomes

This course is part of the **Graduate Certificate in Cyber-security and Risk Management**. Successful completion of this course enables students to meet one or more of the following Program Outcomes:

1. *Identify and map all digital assets to quantify the attack surface and monitor cybercriminal activity. (Reinforce/Master)*
2. *Monitor for threats to organizational digital assets and translate to actionable intelligence. (Introduce)*
3. *Automate actions to block and remove identified threats to digital assets, including integration with other security initiatives in place. (Introduce)*
4. *Manage all components of risk management for successful digital risk protection, including alignment with cyber laws and regulations. (Reinforce/Master)*

Course Outcomes and Module Learning Objectives

This course covers the following specific measurable outcomes and learning objectives. All assessments are aligned to these outcomes and objectives.

Course Outcomes

When you complete this course, you will be able to:

1. Articulate major cybersecurity events and frameworks that have shaped national security and business risk management during the 20th and 21st centuries.
2. Articulate the similarities and differences between a penetration tester/red teamer, cybercriminals, and politically motivated hackers, along with their techniques.
3. Describe the process for conducting cybersecurity risk management based on NIST SP 800-39 and risk assessments based on NIST SP 800-30.

4. Analyze the cybersecurity posture of a Microsoft 365 administrative environment using NIST 800-30 risk assessment methodology and industry-leading practices.

Module Topics and Learning Objectives

The following is a breakdown of module topics and their associated learning objectives.

Module 1: Historical Survey of Cybersecurity Incidents

1. Articulate major historical moments regarding cybersecurity incidents and research (Course Outcome #1)
2. Explain how national security concerns are relevant to cybersecurity ethics (CO1)

Module 2: Risk and Compliance Frameworks Overview

1. Explain relevant cybersecurity governance frameworks (NIST CSF, ISO 27001, NIST 800-30) and regulations (PCI-DSS, GLBA, NERC CIP, CMMC, HIPAA/HiTrust) that apply to various organizations (CO1)
2. Explain how leaders can establish a cybersecurity program using a framework to address relevant regulatory requirements and manage organizational cybersecurity risk (CO3)
3. Articulate the different job functions associated with offensive and defensive cybersecurity operations (CO3)

Module 3: Cybersecurity Actors and Motivations

1. Describe what a penetration test is and the common methods and characteristics of penetration testing (CO2)
2. Describe what a ransomware operation is and the common methods and characteristics of ransomware operations (CO2)
3. Describe what a politically motivated hacker is and the methods and characteristics of so-called “grey hat” hackers (CO2)
4. Perform unauthenticated reconnaissance against a selected organization’s DNS, Microsoft 365, and AWS infrastructure (CO2)

Module 4: Recent Cybersecurity Intrusions

1. Describe common motivations and methods of attackers (CO2)
2. Articulate the significance of Microsoft technologies to modern intrusion techniques, including the significance of phishing for malware execution using LOLBAS (CO2)
3. Analyze business cases related to cybersecurity incidents to identify types of harm incurred (CO1)

Module 5: Techniques & Methods for Assessing Cyber Risk

1. Describe common techniques and methods for assessing cyber risk, including those outlined in the MITRE Att&ck matrix and the NIST Cybersecurity Framework (CSF) (CO3)

2. Describe the difference between qualitative and quantitative cyber risk management processes (CO3)

Module 6: Cyber Attack Case Studies: DFIR & Penetration Testing Reports

1. Analyze a typical incident response report to establish key takeaways (CO4)
2. Analyze common types of penetration testing reports for key risks and prioritized remediation activities (CO4)

Module 7: Cybersecurity Risk Assessment & Executive Reporting

1. Synthesize penetration reports identifying key risks (CO4)
2. Prioritize penetration testing reports results based on risks, available mitigations, and budget constraints (CO5)
3. Report to an executive audience regarding next steps after recent cybersecurity assessment activities (CO5)

Module Learning Materials

Module 1:

Part I: Prior to Trustworthy Computing Memo (1955 – 2002)

a. Multics Security Evaluation: Vulnerability Analysis (Sections 1-3; pgs. 5 – 18 using original pagination)
b. Turing Award Lecture: Reflections on Trusting Trust
c. The Morris Worm: 30 Years Since The First Major Attack On Internet
d. The Morris Worm Videos Part I II III
e. Smashing the Stack for Fun and Profit (pgs. 1-15)
f. L0pht Heavy Industries speaks to US Congress
g. Trustworthy Computing Memo

Part II: After Trustworthy Computing Memo (2003 – Present)

h. Guerilla Open Access Manifesto
i. Darknet Diaries Podcast: Stuxnet
j. Darknet Diaries Podcast: Operation Aurora
k. Aaron Swartz: hacker, genius...martyr?
l. BeyondCorp: A New Approach To Enterprise Security
m. Cybersecurity as RealPolitik
n. Who Are The ShadowBrokers
o. The Solarwinds Orion SUNBURST Attack Timeline and What We Know Now
p. A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack

Module 2:

a. NIST 800-39 – "Managing Information Security Risk"
b. NIST Cybersecurity Framework

c. PCI DSS V4.0
d. PCI DSS SAQ vs. AOC vs. ROC
e. FERPA Guidance
f. Summary of HIPAA Security Rule
g. NIST Guidance on HIPAA Security Rule
h. Updates to GLBA Security Requirements for Financial Institutions
i. CMMC Self-Assessment Guide Level 1

Module 3:

a. Penetration Testing: A Duet
b. How Hackers Hack
c. How We Breached Your Network
d. Darknet Diaries Episode 107 – Alethe
e. Darknet Diaries – Episode 114 – HD
f. Interview with Initial Access Broker Wazawaka
g. An Interview with REvil's Unknown
h. Interview with a L0ckBit ransomware operator
i. Hackback!: DIY Guide for those who can't wait for whistleblowers
j. HackBack!: DIY Guide Second Edition
k. Interview With Phineas Phisher
l. Darknet Diaries: Episode 38 – Dark Caracal
m. Darknet Diaries: Episode 100 – NSO
n. DNS Reconnaissance and User Enumeration Lab

Module 4:

a. Darknet Diaries: Shamoon (Saudi Aramco)
b. Darknet Diaries: Knaves Out (JP Morgan Chase)
c. Darknet Diaries: ShadowBrokers (NSA Tools Leaked) (50 min)
d. Darknet Diaries: Bangladesh Bank Heist (Bangladesh Bank)
e. Darknet Diaries: Dark Basin (WireCard)
f. Darknet Diaries: Triton (Operational Technology Attack)
g. Darknet Diaries: NotPetya (Leaked NSA Tools Used)
h. Darknet Diaries: Wannacry (Leaked NSA Tools Used...Again)
i. Darknet Diaries: REvil
j. Understanding The Threat Landscape with Juan Andres Guerrero-Saade (10 min)
k. LOLBins: Nothing to LOL About (46 min)

Module 5:

a. Virtual Session: NIST Cybersecurity Framework Explained
b. Keynote: Measuring Security Effectively
c. FAIR Cyber Risk Quantification - How Does FAIR Fit Into Your Cyber Strategy?
d. MITRE ATT&CK: The Play at Home Edition (Introduction to MITRE Att&ck)
e. Putting MITRE ATT&CK™ into Action with What You Have, Where You Are

f. Blue Team Keeping Tempo with Offense
g. Tap, Tap, Is This Thing On?
h. Simulating a Cyber Attack – Table-Top Best Practices
i. Backdoors & Breaches: Live Tabletop Exercise Demo
j. 2022 Cyentia Iris Cybersecurity Data Report (3 hrs) (L02)

Module 6:

k. Ryuk in 5 hours – The DFIR Report
l. Emotet Strikes Again: LNK File Leads to Domain Wide Ransomware
m. 2021 Year in Review – The DFIR Report
n. OSQuery Application Security Assessment for Facebook
o. Offensive Security 2013 External + Internal Penetration Test Report
p. Team Project Reference Materials:
   a. Incident Response Report
   b. TCM Security Internal Penetration Test Report Demo Corp
   c. Randori Sec The Hive (Application) Assessment

Module 7:

Based on Team Project Reference Materials from Module 6, develop an over-arching report suitable for an executive audience that analyzes and priorities the remediation of various issues identified across the provided reports. Report analysis should address people resources, organization processes, and technologies/technology configurations that are relevant to the issues at hand.