Term Information

Effective Term	Autumn 2018

General Information

Course Bulletin Listing/Subject Area	International Studies
Fiscal Unit/Academic Org	UG International Studies Prog - D0709
College/Academic Group	Arts and Sciences
Level/Career	Undergraduate
Course Number/Catalog	3702
Course Title	Herding Cyber Cats: Information Security Management
Transcript Abbreviation	Info Sec Mgmt
Course Description	This hands on course will focus on information security governance tools and processes. Students will learn the basic structures and activities used by Information Security professionals to manage information security and cyber risks which threaten us as individuals and organizations.
Semester Credit Hours/Units	Fixed: 3

Offering Information

Length Of Course	14 Week, 12 Week, 8 Week, 7 Week, 6 Week, 4 Week
Flexibly Scheduled Course	Never
Does any section of this course have a distance education component?	No
Grading Basis	Letter Grade
Repeatable	No
Course Components	Lecture
Grade Roster Component	Lecture
Credit Available by Exam	No
Admission Condition Course	No
Off Campus	Never
Campus of Offering	Columbus

Prerequisites and Exclusions

Prerequisites/Corequisites	Sophomore standing or higher, or permission of instructor.
Exclusions	None
Electronically Enforced	No

Cross-Listings

Cross-Listings	None

Subject/CIP Code

Subject/CIP Code	45.0901
Subsidy Level	Baccalaureate Course
Intended Rank	Sophomore, Junior, Senior

Requirement/Elective Designation

Required for this unit's degrees, majors, and/or minors

Course Details

Course goals or learning objectives/outcomes

- Students develop an understanding of the types of cyber security threats to individuals and organizations, and the current laws, regulations and standards prevalent in the discipline.
- Students learn how security programs and tools work to mitigate the threat/impact of cyber threats.
- Students develop and understanding of the roles people, processes and tools play in combating cyber threats, including how the individual can protect him or herself.

Content Topic List

- The Confidentiality-Integrity-Availability (CIA) triad and the Privacy 4th domain.
- Security Threats - Nation-State, Organized Crime, Hacktivists, Insider Threats.
- Security Frameworks and how they relate to managing security: Access, Implement, Monitor, Respond. NIST, ISO, CSA and FISMA standards.
- Governance lifecycles and maturity management.
- Laws and Regulations: HIPAA, FERPA, GLBA, GDPR

Sought Concurrence

No

Attachments

- IS3702_FinalSyllabus.docx

(Syllabus. Owner: Meltz,Richard Lee)

- 1.1 SI_CurriculumMap.docx: Curriculum Map

(Other Supporting Documentation. Owner: Mughan,Anthony)

Comments

- 12/21/17: Please attach a curriculum map which includes 3702 and 4702. *(by Haddad,Deborah Moore on 12/21/2017 04:11 PM)*
- This request is submitted in conjunction with International Studies' proposal to establish a minor in Information Security. *(by Meltz,Richard Lee on 12/21/2017 02:16 PM)*

Workflow Information

Status	User(s)	Date/Time	Step
Submitted	Meltz,Richard Lee	12/21/2017 02:16 PM	Submitted for Approval
Approved	Mughan,Anthony	12/21/2017 02:41 PM	Unit Approval
Revision Requested	Haddad,Deborah Moore	12/21/2017 04:11 PM	College Approval
Submitted	Mughan,Anthony	01/04/2018 10:21 AM	Submitted for Approval
Approved	Mughan,Anthony	01/04/2018 10:22 AM	Unit Approval
Approved	Haddad,Deborah Moore	01/04/2018 02:10 PM	College Approval
Pending Approval	Nolen,Dawn Vankeerbergen,Bernadette Chantal Oldroyd,Shelby Quinn Hanlin,Deborah Kay Jenkins,Mary Ellen Bigler	01/04/2018 02:10 PM	ASCCAO Approval

International Studies 3702
Herding Cyber Cats: Information Security Management

Instructor

Helen Patton

Chief Information Security Officer, Enterprise Security, Office of the CIO

220F Mount Hall

Patton.91@osu.edu

(614) 292-7831

Office Hours: By appointment

Class Time: TBD
Location/Room: TBD

Course Description

This hands on course will focus on information security governance tools and processes. Students will learn the basic structures and activities used by Information Security professionals to manage information security and cyber risks which threaten us as individuals and organizations. This applied knowledge will enable students to understand the context of information security risks in the broader organizational, political and societal contexts.

Course activities will include organizational and threat analysis, creation of continuity, threat mitigation plans, analysis of industry standards and frameworks, and investigation of cyber laws and regulations.

This is a 3 Credit Hour course, lasting 16 weeks, offered in spring of each year. There are no pre-requisites for this course. There is no assigned textbook, and there will be weekly readings drawn from publicly available sources.

Course Goals

By the end of this course, you should be able to understand:

- Types of cyber security threats to individuals and organizations
- Current laws, regulations and standards prevalent in this discipline
- How Security programs and tools work to mitigate the impact of cyber threats to an organization
- The role people, processes and tools play in combating cyber threats
- How to protect yourself from common cyber threats

Course Topics

- Information Security Risk Management Intro - The Confidentiality-Integrity-Availability (C.I.A.) triad, and the Privacy 4th domain
- Security Threats – Nation State, Organized Crime, Hacktivists, Insider Threats
- Security Frameworks – discussion of standard frameworks, how they relate to managing security
    - Assess, Implement, Monitor, Respond
    - NIST, ISO, CSA, FISMA
- Data Management Planning
- Governance lifecycles and maturity management
- Laws and Regulations – HIPAA, FERPA, GLBA, GDPR, etc.
- Organizational Policies and Strategies – Acceptable Use, Data Management Policies, and Training Options
- Assessing Risk in an Enterprise – where to focus efforts, where to accept risk
- Business Continuity and Disaster Recovery planning for people, process and tools
- Stakeholder Engagement, reporting and metrics for Risk
- Emerging trends: Cloud, Internet of Things (IOT), Big Data, Digital Identities
- Strengths and weaknesses of Security accreditation and certification

Required Readings

Students will be expected to read all materials (freely available online readings, case studies, policies and other texts) assigned by the instructor. Their knowledge and understanding of the material will be evaluated through the course journal, presentation, written assignments and in class discussions.

Students will be expected to stay abreast of current events related to Information Security. This can be readily done by (e.g.) a daily review of online newspapers, e.g. *The New York Times*, etc. and online magazines e.g. *https://www.csoonline.com/*. Students will be introduced to sources the first week of class. Student knowledge and comprehension of current events will be evaluated through participation in class discussions. For each class session, students should be prepared to share with the class the current event that has occurred within the past few days that they think is particularly noteworthy.

Course Strategy and Structure

The course will provide a broad overview of Information Security management, as it has developed since this century. However, the subject matter of this course is constantly evolving. As such, considerable attention will be given to discussing current events and case studies during the course. As needed, the instructor will adjust the schedule of topics to be discussed during the course, to take advantage of changing circumstances and contemporary issues. The course schedule might also be modified to take advantage of the unforeseen availability of guest experts.

The course will employ a number of learning mechanisms to accomplish the course objectives, including:

- Lectures by the course instructor
- Lectures by guest speakers
- Discussions of various topics and issues, guided by the instructor and/or students; and
- Presentations by students

Course Assignments/Grading

Grades will be assigned according to the following scheme:

Evaluation	**Points**	**Due**	**% of Grade**
Personal Threat Analysis	20	Week 4	10
Create a Data Management Plan	30	Week 9	15
Create a BC plan	30	Week 13	15
Create a Personal Learning Plan	20	Week 14	10
Reflection Journal	10	Week 6 & 15	5
Cyber Law/Regulation Presentation	40	TBD	20
Participate in Tabletop exercise	10	Week 14	5
Table Top Lessons Learned	30	Week 16	15
Attendance	10	All	5
Total Points In Course	**200**		

Grading Scale:

A	93-100%
A-	90-92%
B+	87-89%
B	83-86%
B-	80-82%
C+	77-79%
C	73-76%
C-	70-72%
D+	67-69%
D	60-66%
E	0-59%

Course Policies

Attendance and Participation

Attendance is critical in this class and will be taken daily. If you forget to check-in you could lose your attendance point for that day.

Please let the instructor know before class or within 48 hours of missing the class (via email is fine). Additionally, if you miss a class you are responsible for getting notes and information missed from your fellow classmates.

Writing

All assignments to be written in 12-point font with 1-inch margins. Everything should be double-spaced and should always include a title, your name, the date, and the course. Writing is a tool that allows us to express ourselves throughout our lives. If you need assistance, do not be afraid to ask your instructor or consult a university resource, such as the Writing Center, which offers free tutorials on writing

Make-up Presentations

Make-up presentations will be arranged for university-excused or unavoidable circumstances (e.g., deaths, personal/family illness and emergencies) with prior notification or written verification within 72 hours of your absence. If you are not present in a class during an exam or presentation, and you do not have the proper documentation, you will not be allowed to make it up.

Late Work

Assignments should be handed in on time. However, we understand that situations occasionally come up. We are generally not concerned if an assignment is a few hours late, but if your assignment is more than a day late it will be graded for full credit only in situations where (1) the assignment was late due to unavoidable circumstances and (2) you let the instructor know about your situation within 48 hours of missing the deadline. If you do not turn something in and you don't communicate with your instructor within 48 hours of missing the deadline, you will receive zero points.

Grade Disputes

We are happy to revisit grades and to discuss the evaluation of your work with you. Grade change requests can be made in-person or via email. Please be ready to outline where you believe you should have received additional points and how many points you should have received.

Plagiarism

All work in this course is to be individually developed. Plagiarism includes using another person's writing without giving them credit, using large verbatim sections of the work of another person or online source (even a public source) or submitting something you have written for another class. If you unsure, please give credit to your source or talk to your instructor about it. Students who plagiarize will be penalized and reported to university officials. You will also receive a grade of zero for the assignment where plagiarism occurred.

Academic Misconduct

Academic integrity is essential to maintaining an environment that fosters excellence in teaching, research, and other educational and scholarly activities. Thus, The Ohio State University and the Committee on Academic Misconduct (COAM) expect that all students have read and understand the University's *Code of Student Conduct*, and that all students will complete all academic and scholarly assignments with fairness and honesty. Students must recognize that failure to follow the rules and guidelines established in the University's *Code of Student Conduct* and this syllabus may constitute "Academic Misconduct."

The Ohio State University's *Code of Student Conduct* (Section 3335-23-04) defines academic misconduct as: "Any activity that tends to compromise the academic integrity of the University, or subvert the educational process." Examples of academic misconduct include (but are not limited to) plagiarism, collusion (unauthorized collaboration), copying the work of another student, and possession of unauthorized materials during an examination. Ignorance of the University's *Code of Student Conduct* is never considered an "excuse" for academic misconduct, so I recommend that you review the Code of Student Conduct and, specifically, the sections dealing with academic misconduct.

If I suspect that a student has committed academic misconduct in this course, I am obligated by University Rules to report my suspicions to the Committee on Academic Misconduct. If COAM determines that you have violated the University's *Code of Student Conduct* (i.e., committed academic misconduct), the sanctions for the misconduct could include a failing grade in this course and suspension or dismissal from the University.

If you have any questions about the above policy or what constitutes academic misconduct in this course, please contact me.

DisabilityServices

The University strives to make all learning experiences as accessible as possible. If you anticipate or experience academic barriers based on your disability (including mental health, chronic or temporary medical conditions), please let me know immediately so that we can privately discuss options. To establish reasonable accommodations, I may request that you register with Student Life Disability Services. After registration, make arrangements with me as soon as possible to discuss your accommodations so that they may be implemented in a timely fashion. SLDS contact information: slds@osu.edu; 614-292-3307; slds.osu.edu; 098 Baker Hall, 113 W. 12th Avenue.

Statement on Diversity

The Ohio State University embraces and maintains an environment that respects diverse traditions, heritages, experiences, and people. Our commitment to diversity moves beyond mere tolerance to recognizing, understanding, and welcoming the contributions of diverse groups and the value group members possess as individuals. The faculty, students, and staff are dedicated to building a tradition of diversity with principles of equal opportunity, personal respect, and the intellectual interests of those who comprise diverse cultures.

Class Schedule

Week (SP18)	Dates	Topic	Readings (under development)	Assignments Due
Security Strategies and Influences				
1 – Jan 8	Day 1	Course overview & syllabus • Creating a Reflections Journal	Syllabus	None
	Day 2	Finding resources for Information Security – Security communities (Professional and Personal)	Investigate Security Sources	**Bring examples of Security Sources to class**
2 – Jan 15	Day 1	Intro to Cyber Risk Management – the CIA Triad and the role of Privacy	*Target* Use Case The CIA Secret https://www.sagedatasecurity.com/blog/fundamental-objectives-of-information-security-the-cia-triad 11 Simple Ways to Protect Your Privacy	
	Day 2	Creating Data Management Plans for work and personal use • Mid Term Assignment Overview	OSU Data Management Plans Ten Simple Rules for Creating a Good Data Management Plan How to Keep Your Personal Information Secure Data Protection Tips	Presentation: CFAA
3 – Jan 22	Day 1	Security Threats - Nation State, Organized Crime, Hacktivists, Insider Threats *Guest speaker re: Nation State threat	Threat Actor Types Overview of Threat and Risk Analysis	
	Day 2	Creating a Personal Threat Analysis	Creating a Personal Threat Analysis Creating a Threat Profile for your Organization Personal Threat Models	Presentation: HIPAA

4 – Jan 29	Day 1	Cyber Compliance - Laws and Regulations • How difference Business sectors respond to compliance issues	US Cyber Law Summary Cyber Security Regulatory Crackdown RSA Cyber Laws and Responsibilities Data Protection in the United States - Overview	**Personal Threat Analysis**
	Day 2	Risk Tolerance – understanding decision making	Cyber Risk Appetite How to understand your risk tolerance What is Your Risk Appetite? Naomi Klein Addicted to Risk	Presentation: PCI
5 – Feb 5	Day 1	Organizational Policies and Compliance • Difference between policies, standards and procedures • Roles & Responsibilities across an organization	OSU Policies Describing Policies, Standards, Guidelines and Procedures Policy Hierarchy FFIEC IT Examination – Roles & Responsibilities	
	Day 2	User expectations of company management of data	*Equifax* use case *Equifax* case study Executive Expectations Consumer Expectations Millennial Expectations Regulator Expectations	Presentation: GDPR
6 – Feb 12	Day 1	Security Frameworks - Assess, Implement, Monitor & Respond • Understanding when/how standards are used • Understand elements of a framework • Understand value in organizational change	NIST Framework NIST vs. ISO Frameworks	**Reflections Journal (part 1) due**

		management		
	Day 2	Implementing governance lifecycle into Data Management Plans	ISACA Governance lifecycles MITRE Cyber Security Governance	Presentation: GLBA
7 – Feb 19	Day 1	Data Classifications models • What is asset classification • Sensitivity vs. Criticality • Risk vs. Impact	OSU IDP Policy and Data Classifications CISSP Classifying Data	
	Day 2	Classifying Data for Data Management Plans	Berkeley Data Classification Standard USF Sensitivity and Criticality of Data	Presentation: FERPA
8 – Feb 26	Day 1	Emerging Trends in Security – Cloud, IOT, Big Data, Identity Management	*AWS* Use Case MIRAI Botnet Use Case Ecosystem Risk Big Data Risk	
	Day 2	Security's relationship to other corporate functions: Finance, HR, Law, Facilities, Internal Audit, etc.	Internal Audit's role in Cyber Security The role of HR in mitigating Cyber Security threats	Presentation: Ohio Breach Notification
9 – Mar 5	Day 1	Creating a Security Business Case • Why a Bus. Case is needed, when they are used • Elements of a Bus. Case	4 Steps to a Perfect Business Case Building a business Case for Information Security	
	Day 2	Optional Class for questions	Mid Term Exams week	**Data Management Plan Due**
Influencing People and Behaviors				
10 – Mar 12	Day 1	No Class	Spring Break	
	Day 2	No Class	Spring Break	
11 – Mar 19	Day 1	Business Continuity Planning Basics Part 1 • What are BC plan elements	Creating an effective business continuity plan 7 Key elements of business continuity	
	Day 2	Writing a BC Plan *Guest speaker re: BC Planning	12 Attributes of a Successful BC Plan	Presentation: FISMA
12 – Mar 26	Day 1	Business Continuity	BC Scenarios	

		Planning Basics Part 2 • BC Scenarios • Table top exercises	Types of Exercises	
	Day 2	Writing a BC Plan • 3rd Parties • Communications	Crisis Communications BC Plans and 3rd Parties	Presentation: COPPA
13 – Apr 2	Day 1	Security Training and Awareness • Training others • Certifications/Training for practitioners *Guest Speaker re: Training	Importance of Security Awareness Training Security Certifications you should have Cyber Security Certifications	**BC Plan Due**
	Day 2	Class Discussion: Phishing Awareness	FTC Phishing Information	Presentation: ITAR
14 – Apr 9	Day 1	**Participate in Table Top Exercise**		**Learning Plan Due**
	Day 2	**Debrief Table Top Exercise**		
15 - Apr 16	Day 1	Reporting and Metrics for Risk • Strategic vs. management metrics • KGIs, KPIs and KRIs • How to communicate throughout the enterprise	Board Level Cyber Metrics KPIs and KRIs	**Reflections Journal**
	Day 2	More Metrics	Amazon Dashboard	
16 – Apr 23	Day 1	Optional Class for questions	Final Exams Week	**Table Top Lessons Learned and updated BC/DR Plan Due**

Curriculum map, indicating how program goals are accomplished via specific courses

Security & Intelligence Specialization MAP	LEARNING GOALS					
	Program				Specialization	
	A	B	C	D	E	F
	Key: 1=Beg. 2=Int. 3=Adv.					
Required Pre-Major Courses: 6-18 hours						
History 2550		1	1	1	1	
Psychology 1100		1		1		
Completion of 1103	1	1		1		
1. REQUIRED FOUNDATION: 12 hours						
Introduction to Intelligence 3700		2	2	2	2	2
International Studies 4700		3	3	3	3	
Political Science 4315		3	3	3	3	
Psychology 4525		2	2	2	2	
2. CRITICAL PERSPECTIVES: (choose four) 12 hours						
Earth Sciences 3411		2	2	2	2	
Economics 4547		3	3	3	3	
Geography 3300		2	2	2	2	2
History 3540		2	2	2	2	2
History 3552		2	2	2	2	
History 4550		3	3	3	3	3
International Studies 3701		2		2	2	2
International Studies 3702		2		2	2	2
International Studies 4251		3	3	3	3	
International Studies 4532		3	3	3	3	
International Studies 4550		3	3	3	3	
International Studies 4701		3	3	3	3	
International Studies 5700		3	3	3	3	
International Studies 5701E		3	3	3	3	3
International Studies 5702		3	3	3	3	
International Studies 5703		3	3	3	3	3
Linguistics 3801		2		2	2	
Political Science 4310		3	3	3	3	
Political Science 4318		3	3	3	3	
Sociology 3315		2	2	2	3	
Sociology 5525		3	3	3	3	3
3. ELECTIVES: Choose two: 6 hours						
Anthropology 3211		2		2	2	
Anthropology 3305		2		2	2	
Communication 3597.02		2	2	2	2	
Computer Science & Eng. 4471		3		3	3	3
Earth Sciences 4425		3		3	3	
Economics 3790		2	2	2	3	
Environ. & Natural Resources 4648		3		3	3	
Geography 5200		3		3		3
Geography 5300		3		3	3	
History 3270		2	2	2	2	
History 3551		2	2	2	2	
History 3560		2	2	2	2	
History 3561		2	2	2	2	

History 3570		2	2	2	2	
History 3580		2	2	2	2	
International Studies 3400		2		2		
International Studies 4703		3	3	3	3	
International Studies 4803		3	3	3	3	
International Studies 4998		3	3	3	3	3
International Studies 4999		3	3	3	3	3
International Studies 5191		3		3	3	3
International Studies 5195		3		3	3	3
International Studies 5797		3	3	3	3	
Sociology 3410		2	2	2	2	2
Sociology 5618		3		3	3	3
1. **COMPLETION OF A FOREIGN LANGUAGE MINOR.**	3	3		3		

PROGRAM LEARNING GOALS:

A. Students are competent in a foreign language.
B. Students complete a rigorous liberal arts education that is international in focus and prepares them for a range of careers.
C. Students understand the diversity of influences-historical, economic, political, social and cultural-that shape domestic and international processes and outcomes.
D. Students master critical reasoning and cross-cultural communications skills.

SPECIALIZATION LEARNING GOALS:

E. Students develop an interdisciplinary understanding of the threats to the security and well-being of states and their peoples.
F. Students examine states' response to these threats by gathering, analyzing and disseminating intelligence information.