

Fiscal Unit/Academic Org	UG International Studies Prog - D0709
Administering College/Academic Group	Arts and Sciences
Co-administering College/Academic Group	
Semester Conversion Designation	New Program/Plan
Proposed Program/Plan Name	Information Security
Type of Program/Plan	Undergraduate minor
Program/Plan Code Abbreviation	INFOSEC
Proposed Degree Title	Information Security

Credit Hour Explanation

Program credit hour requirements		A) Number of credit hours in current program (Quarter credit hours)	B) Calculated result for 2/3rds of current (Semester credit hours)	C) Number of credit hours required for proposed program (Semester credit hours)	D) Change in credit hours
Total minimum credit hours required for completion of program				16	
Required credit hours offered by the unit	Minimum			6	
	Maximum			6	
Required credit hours offered outside of the unit	Minimum			4	
	Maximum			4	
Required prerequisite credit hours not included above	Minimum			14	
	Maximum			16	

Program Learning Goals

Note: these are required for all undergraduate degree programs and majors now, and will be required for all graduate and professional degree programs in 2012. Nonetheless, all programs are encouraged to complete these now.

Program Learning Goals

- Students acquire an understanding of the nature of cyber threats to the security, integrity, and availability of digitalized information as well as of the laws, regulations and standards designed to counter these threats.
- Students understand such information security procedures as intrusion detection, risk management framework management, penetration testing and identity and access management through the analysis of case studies and personal reflection.
- Through exposure to computer programming coursework, students develop an understanding of computer network security issues.
- Students gain an understanding of the social contexts in which information security issues arise, including organized crime, inter-state relations and insider threats.

Assessment

Assessment plan includes student learning goals, how those goals are evaluated, and how the information collected is used to improve student learning. An assessment plan is required for undergraduate majors and degrees. Graduate and professional degree programs are encouraged to complete this now, but will not be required to do so until 2012.

Is this a degree program (undergraduate, graduate, or professional) or major proposal? No

Program Specializations/Sub-Plans

If you do not specify a program specialization/sub-plan it will be assumed you are submitting this program for all program specializations/sub-plans.

Pre-Major

Does this Program have a Pre-Major? No

Attachments

- InfoSecProposal_Final.pdf
(Program Proposal. Owner: Mughan,Anthony)
- InfoSec_AdvisingSheets.pdf
(Semester Advising Sheet(s). Owner: Mughan,Anthony)
- InfoSec_3702&4702Syllabi.pdf: Syllabi
(Other Supporting Documentation. Owner: Mughan,Anthony)
- Formal Concurrences.docx
(Support/Concurrence Letters. Owner: Mughan,Anthony)

Comments

- As part of this request, two new courses have to be approved INTSTDS 3702 and INTSTDS 4702. A syllabus for each of them is attached. *(by Mughan,Anthony on 12/19/2017 11:05 AM)*

Workflow Information

Status	User(s)	Date/Time	Step
Submitted	Mughan,Anthony	12/19/2017 11:05 AM	Submitted for Approval
Approved	Mughan,Anthony	12/19/2017 11:06 AM	Unit Approval
Approved	Haddad,Deborah Moore	12/19/2017 03:13 PM	College Approval
Pending Approval	Nolen,Dawn Vankeerbergen,Bernadette Chantal Oldroyd,Shelby Quinn Hanlin,Deborah Kay Jenkins,Mary Ellen Bigler	12/19/2017 03:13 PM	ASCCAO Approval

PROPOSAL FOR A MULTIDISCIPLINARY B.S. MINOR IN INFORMATION SECURITY

To: ASC Curriculum Committee

From: Anthony Mughan, Director, Undergraduate International Studies Program (UISP)

Date: 8 November, 2017

Background

Human knowledge is based on information and the data generated from it. As today's world has become more complex, technology more advanced and states more interdependent, ready-to-hand information on all facets of human existence is unprecedented in its diversity and volume. Moreover, whether it relates to national economic strategy, corporate product development, advanced weapons research, or whatever, much of this information has great economic and/or strategic value to competitors as well as its owners. Protecting information, therefore, is, and has long been, a major preoccupation for a wide array of actors, including governments, research agencies, institutions of higher education, corporations, and marketers. Their goals include not only keeping it safe from competitors, but also maintaining its integrity against efforts to corrupt it as well as ensuring its availability to targeted consumers in the face of ransomware or denial of service attacks. In one sense, of course, nothing is new here. Nations, corporations and private individuals have long employed technology, spies and insiders to steal intellectual property, ranging from customer/sales data to fully articulated weapons system blueprints. Those at the receiving end of such activities have, needless to say, responded by going to great lengths to protect their assets.

Thus, there is nothing new in the need to keep certain information secure, but what is new is that today's world has witnessed perhaps unprecedented change in the information security environment. While the filing cabinet, lockbox and safe remain important means of storing physical manifestations of information, more and more the means of storage is digital (whether local or in the Cloud) which means that it can be accessed remotely. This makes for a very different, and challenging, information security environment. Digitalized personal, private and public systems have become unprecedentedly interconnected and at the same time cheap, adaptable technology is now readily available to an array of national and international actors intent on breaching information defences for personal or national advantage. Immense damage and disruption can ensue. For example, basic infrastructure (power, water, food production, transport, and the like) is increasingly managed digitally, making effective information security a matter of national survival as well as security. The stakes for individuals can also be high. Breaches of their privacy may go undetected for some time and the harm done to them may be all the more severe for this delay.

For all these reasons, protecting the integrity of systems that collect, house and transmit information and data has become an unprecedentedly complex preoccupation for many in the modern, “internet-enabled” world.

Rationale

Information security is not only a practice, but also an emergent and increasingly diverse field of academic study. Lying at the heart of the data protection enterprise commonly known as cybersecurity, the study of information security addresses broad issues relating to the confidentiality, integrity and availability of information and data. Topics covered include risk and its management, ethics, law, policy and education. In this sense, the study of information security functions as a necessary background to more technical discussions of the mechanics of data protection once digitalized. Generally known as cybersecurity, these discussions focus largely on the role of computers and computing in promoting information security. Thus, the just-introduced bachelor’s degree in cybersecurity at the University of Akron promises that “(s)tudents in the cybersecurity track will learn about computer network configuration, computer network and data security, network intrusion prevention and detection, as well as computer networking forensics and digital forensics” (*Akron Beacon Journal*, June 21, 2017).

The minor that we are proposing starts from the premise that the information security enterprise is about more than just computers and computing. At a minimum, core issues relating to the confidentiality, integrity and confidentiality of information and data need to be addressed and understood, albeit perhaps as a prelude to a more specialized focus on the mechanics of keeping information safe once digitalized. But this proposed minor also recognizes that understanding and countering challenges to information security must take account of the larger social, economic and security environment in which threats emerge and crystallize. It is, in other words, a necessarily multi-disciplinary endeavor. Cybersecurity educators widely acknowledge that “(h)acking is a crime that involves creativity, an understanding of human behavior, and expertise in the full range of endeavors that involve computers.” Thus, “even for institutions still focused mainly on teaching (computer) code, extensive worker shortages mean that cybersecurity graduates will find jobs, especially if they come with a solid liberal-arts education. Companies are accustomed to taking entry-level workers with raw ability and teaching them additional skills specific to their jobs” (*Chronicle of Higher Education*, March 23, 2017).

Ohio State is well-placed to offer a first-class minor in Information Security because of the faculty expertise and the breadth and depth of relevant courses on which it can draw. Moreover, all involved in the new minor will be better off for its being in existence. Take the University itself, for example. With the minor’s topicality and profound implications for personal and national security, as well as for our understanding and management of patterns of international cooperation and conflict, it amply fulfils one of the core missions of The Ohio State University, which is to create and discover knowledge to improve the well-being of our state, regional, national and global communities. The student body also has the potential to draw great benefit from it. The minor has been designed with the curricular needs of the multi-disciplinary International Studies program in mind, and especially those of its students choosing the BS *Security & Intelligence* specialization. It should, however, also appeal to students across the University, and especially those in the Colleges of Business and Engineering. In addition, at the

same time as enriching the curricular choices available to undergraduate students, the minor could well help prepare them better for the labor market after graduation or for graduate work in high-quality programs like Carnegie-Mellon's *Master of Science in Information Security Policy and Management* or Johns Hopkins University's *Master of Science in Security Informatics*.

Curriculum

The proposal is for a 16-hour multi-disciplinary minor in Information Security. All students will take four required courses, which must be passed with a grade of C-, or higher. The first (CSE 2501) is a general introduction to the major social, ethical and professional issues involved in computing. Then comes another general introductory course, this time on the subject of information security management. Students have to pass both these introductory courses to be able to proceed to take the two remaining required courses CSE 4471 and INTSTDS 4702. CSE 4471, in turn, is a prerequisite for INTSTDS 4702 and they introduce students to the study of computer networks and data security on the one hand and they cover strategies, processes, and tools aimed at preserving the confidentiality, integrity and availability of information and the systems used to store and process it on the other. The remaining six credit hours will be satisfied by choosing two courses from a set of electives that essentially places the pursuit of information security in a broader economic, social and security context involving considerations of espionage, global crime, ethical dilemmas, and the like. To be precise, the proposed curriculum is:

Required Courses (10 hours)

Computer Science and Engineering 2501: Social, Ethical and Professional Issues in Computing (1 credit hour)

International Studies 3702: Herding Cyber Cats: Information Security Management (3 credit hours)

Computer Science and Engineering 4471: Information Security (3 credit hours)

International Studies 4702: Case Studies in Information Security (3 credit hours)

Electives (6 hours)

Communication 3332: Risk Communication (3 credit hours)

Computer Science and Engineering 5351: Introduction to Cryptography (3 credit hours)

Computer Science and Engineering 5473: Network Security (3 credit hours)

International Studies 3700: Introduction to Intelligence (3 credit hours)

International Studies 3701: Introduction to Homeland Security (3 credit hours)

International Studies 5191: Internship (3 credit hours)

Linguistics 3801: Code Making and Code Breaking (3 credit hours)

Linguistics 3802: Language and Computers (3 credit hours)

Public Affairs 4000: Public Policy Evaluation (3 credit hours)

Sociology 5525: Global Criminology (3 credit hours)

Course Synopses

Required

<p>Computer Science and Engineering 2501: <i>Social, Ethical and Professional Issues in Computing</i></p>	<p>Social, ethical, and professional issues facing computing professionals; ethical principles; discussion of case studies.</p>	<p>Prereqs: CSE 2122 or CSE 2123 or CSE 2231, and a Gen Ed Writing Level 2.</p>
<p>International Studies 3702: <i>Herding Cyber Cats: Information Security Management</i></p>	<p>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</p>	<p>Prereq: None</p>
<p>Computer Science and Engineering 4471: <i>Information Security</i></p>	<p>Introduction to security of digital information; threats and attacks; regulations; risk management; attack detection and response; cryptography; forensics; technical training and certifications</p>	<p>Prereq: CSE 2122 or CSE 2123 or CSE 2231</p>
<p>International Studies 4702: <i>Case Studies in Information Security</i></p>	<p>This course will provide students with a deeper understanding of core elements of Information Security through review and analysis of real-world case studies, security frameworks, annual trend/survey reports and related materials.</p>	<p>Prereqs: INTSTDS 3702, and CSE 4471</p>

Electives

<p>Communication 3332: <i>Risk Communication</i></p>	<p>Students will learn how to plan, implement and evaluate a risk communication effort. Message design is an integral part of this class.</p>	<p>Prereq: Not open to students with credit for 632.</p>
<p>Computer Science and Engineering 5351: <i>Introduction to Cryptography</i></p>	<p>Foundations of cryptography, mathematical formulations/proofs of security goals; theory and practical constructions of encryption schemes, MACs, digital signatures; zero-knowledge proof systems; cryptographic protocols.</p>	<p>Prereqs: CSE 2331 (680), CSE 5331, Math 4573 (573), or Math 4580 (580), and Stat 3460 (427) or 3470.</p>
<p>Computer Science and Engineering 5473: <i>Network Security</i></p>	<p>Security threats and services, elements of cryptography, protocols for security services, network and internet security, advanced security issues and technologies.</p>	<p>Prereq: CSE 3461 (677) or CSE 5461.</p>
<p>International Studies 3700: <i>Introduction to Intelligence</i></p>	<p>Comprehensive introduction to the gathering, analysis, and use of military and political intelligence in a number of countries.</p>	<p>Prereq: None.</p>
<p>International Studies 3701: <i>Introduction to Homeland Security</i></p>	<p>Comprehensive overview of U.S. homeland security. Threats from natural disasters, terrorism, and other domestic and external sources will be studied, as will programs and technologies involved in disaster prevention and response.</p>	<p>Prereq: Soph standing or higher.</p>
<p>International Studies 5191: <i>Internship</i></p>	<p>Opportunity to gain knowledge of the policy process in a local, national international or government agency.</p>	<p>Prereq: GPA 3.0 or above, and Jr. or Sr. or Grad standing. Graded S/U.</p>
<p>Linguistic 3801: <i>Code Making and Code Breaking</i></p>	<p>Introduction to old and new technology associated with</p>	<p>Prereq: None</p>

	codes and code-breaking and the ways in which it has impacted people's lives.	
Linguistic 3802: <i>Language and Computers</i>	Introduction to human language technology, explaining the computational and linguistic principles behind such familiar technologies as web search, machine translation, and spelling correction.	Prereqs: Soph standing or above. GE quant reason math and logical analysis course.
Public Affairs 4000: <i>Public Policy Evaluation</i>	The purpose of this course is to develop and apply research design and analytic methods to public policy evaluation. The course will enable students to design and perform policy evaluations focused on policy processes and outcomes, using both qualitative and quantitative data.	Prereqs: PubAfrs 3000, Stat 1350 or above, and Econ 2001.01 or equiv, or permission of instructor.
Sociology 5525: <i>Global Criminology</i>	Provides students with an introduction to global crime from a criminal justice perspective.	Prereq: Jr., Sr. or Grad standing, or permission of instructor or department.

This minor has been planned as an addition to the list of minors approved for students pursuing the BS version of the International Studies major. However, it will also be open to all members of Ohio State's undergraduate student body.. No more than one course in it will be allowed to count towards the IS major. Two of the courses required in this minor (INTSTDS 3702 and INTSTDS 4702) are being submitted for approval at the same time as is the minor as a whole. All its elective courses are approved and already on the books; they are also generally taught by faculty in the departments offering them. Students must maintain a C average in the minor, and no grade lower than C- will count towards the minor.

Administration

Although this minor is a joint venture with Office of the Chief Information Officer, the academic home of this minor is the Undergraduate International Studies Program and it will be listed in the OSU Bulletin as "a multidisciplinary minor offered by the Undergraduate International Studies Program." Individual departments will not be listed so as to allow for the addition and subtraction of courses as circumstances in the contributing units change and/or as new units choose to list courses in the minor. To declare a minor, students will meet with a UIISP advisor,

with whom they will plan their minor program. Proposed curriculum changes to the minor will be discussed by the Steering Committee that created it ((Anthony Mughan, Director of International Studies, Helen Patton (Chief Information Security Officer), and Steve Romig (Director-Security Advisor)) and referred to the UISP Oversight Committee for approval.

Departments wishing to propose courses for the Information Security minor should submit the following to the UISP Director:

- A fully articulated syllabus for the course(s);
- A statement (two pages maximum) describing how the proposed course(s) would add to the Information Security minor;
- A description of the history of the proposed course – i.e., is it new? How many times has it been offered before and how often will it be offered in the future?
- A short biography of the faculty member who will have primary responsibility for teaching the course

All the courses that figure, now or in the future, in the proposed minor will have to share the characteristics of being offered regularly, preferably once a year but no less than once every two years.

Competition

In the state of Ohio, a number of community colleges (e.g., Columbus State and Stark State) have two-year cybersecurity programs and Kent State University offers a post-secondary certificate in Computer Forensics and Information Security. As for four-year degrees, three universities offer a major in the general area of cybersecurity, all of which have an overwhelming computer science emphasis. Ohio State offers an Information Security focus within its BS in Computer Science and Engineering, the University of Akron has just introduced a BS degree in cybersecurity, and Tiffin University offers a BS in Cyber Defense and Information Assurance.

A good number of similar programs can be found in surrounding states. The University of Charleston in West Virginia, for example offers a BS in Cyber Security, while the University of Pittsburgh is similar to Ohio State in that it has a Networks and Security specialization within its BS in Information Sciences. The state of Michigan has a number of programs, including an Information Assurance major at Eastern Michigan University and a BS in Cybersecurity and Information Assurance at the University of Michigan-Dearborn. A fuller listing can be found at cyberdegrees.org.

What distinguishes our proposed Information Security minor from these other programs is its multi-disciplinary character, its goal of placing the study of information security in its economic, social and security context as well as within the broader framework of a first-class liberal arts education. For those who wish to pursue a career in cybersecurity, it is designed to provide a solid conceptual and technical foundation for the acquisition of the advanced computer skills that they will need.

Expected Student Enrollment

Year 1: 15 students

Year 2: 30 students

Year 3: 50 students

Implementation of Proposed Minor

Letters of concurrence from the heads of contributing departments are attached to this proposal (see Appendix A). It is hoped that the proposal will be approved by both ASC Curriculum Committee and CAA by the end of the 2018 Spring semester so that implementation will be possible in Autumn 2018.

Questions regarding this proposal should be addressed to Anthony Mughan, 33 Townshend Hall, 1885 Neil Avenue, CAMPUS; his telephone number is 292-9657 and his e-mail address is mughan.1@osu.edu.

International Studies 3702

Herding Cyber Cats: Information Security Management

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

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

- 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 are 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.

Disability Services

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 <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> Difference between policies, standards and procedures 	OSU Policies Describing Policies, Standards, Guidelines and Procedures Policy Hierarchy FFIEC IT Examination – Roles & Responsibilities	

		<ul style="list-style-type: none"> Roles & Responsibilities across an organization 		
	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 <ul style="list-style-type: none"> Understanding when/how standards are used Understand elements of a framework Understand value in organizational change management 	NIST Framework NIST vs. ISO Frameworks	Reflections Journal (part 1) due
	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 <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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 Planning Basics Part 2 <ul style="list-style-type: none"> BC Scenarios Table top exercises 	BC Scenarios Types of Exercises	
	Day 2	Writing a BC Plan <ul style="list-style-type: none"> 3rd Parties Communications 	Crisis Communications BC Plans and 3rd Parties	Presentation: COPPA
13 – Apr 2	Day 1	Security Training and Awareness <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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
--	--	--	--	---------------------------

International Studies 4702

Case Studies in Information Security

Spring 2019

Short Description

This course will provide students with a deeper understanding of core elements of Information Security through review and analysis of real-world case studies, security frameworks, annual trend/survey reports and related materials.

Course Description

The goal of this course is to provide students who have taken an introductory Information Security course (such as CSE 4471) with a more advanced understanding of the background, terminology, and concepts of Information Security. This will prepare students to engage in deeper study of Information Security and to apply what they have learned in business and technical contexts.

This course will focus heavily on behavioral outcomes demonstrating the ability to use knowledge gained in an introductory course, such as developing security requirements from business use-cases, comparing security requirements against implementation reality, and conducting post-incident reviews.

Course material will be drawn from real world events such as Stuxnet, SONY Pictures, Target, and EquiFax; emerging information technologies such as Social Media, Cloud Computing, Big Data and the Internet of Things; and perennial concerns such as privacy, public safety and business considerations.

This is a 3 Credit Hour course, lasting 14 weeks, offered in Spring of each year. There is no assigned textbook: weekly readings drawn from publicly available sources.

Pre-Requisites

CSE 4471, "Introduction to Information Security"

International Studies 3702, "Herding Cyber Cats"

Course Goals

By the end of this course, you should have a deeper understanding of the following topics using case studies and real-world examples:

- The application of a variety of security controls to address risk based on real-world examples
- Threats, with a focus on organized crime and nation-states
- Intrusion detection, threat hunting and incident response/investigations
- Penetration testing
- The underground economy
- Vulnerability, patch and related service management areas
- Identity and access management
- Inside threats and user behavior analytics

Instructor

Steve Romig, Office
of the CIO

Mount Hall

romig.1@osu.edu

(614) 688-3412

Office Hours: TBD

Class Time: T/Th

Location/Room: TBD

Required Readings

See Schedule Below

Course Assignments and Grading

The course will require weekly reading, including identification of “current events” for discussion online and in class.

Grading for the course will be largely based on participation in on-line and in-class discussions and on four individual and group projects where students research, analyze and present case studies and other detailed analysis relating to the material discussed in class. This will include one or two short (15-20 minute) presentations in class.

Sample reading assignments:

- Ken Thompson, “Reflections on Trusting Trust”, Turing Award Lecture, Association for Computing Machinery, August 1984, <http://dl.acm.org/citation.cfm?id=358210>
- Jason Franklin, Adrian Perrig, Vern Paxson, Stefan Savage, “An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants”, CCS, 2007, <http://www.icir.org/vern/papers/miscreant-wealth.ccs07.pdf>
- Peter Loscocco, Stephen Smalley, Patrick Muckelbauer, Ruth Taylor, S. Jeff Turner, John Farrell, “The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments”, 21st National Information Systems Security Conference, October 1998, <https://www.cs.utah.edu/flux/fluke/html/inevit-abs.html>
- “Verizon’s 2017 Data Breach Investigations Report”, May 2017, <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>
- Center for Internet Security (CIS) Benchmark, <https://www.cisecurity.org/cis-benchmarks> (license required, available through OSU Enterprise Security)
- OSU Computer Security web site: <https://cybersecurity.osu.edu/>
- OSU Information Security Standard (ISS): <https://go.osu.edu/infosec-iss> (OSU login required)
- OSU Information Security Control Requirements (ISCR): <https://go.osu.edu/infosec-iscr> (OSU login required)
- Material on Stuxnet, such as the book “Countdown to Zero Day” by Kim Zetter or the documentary “Zero Days” directed by Alex Gibney.
- Material relating to security incidents such as the 2013 Target breach, the 2014 Home Depot breach, the 2014 Sony Pictures breach, the 2016 DNC breach and so on.

Papers/Presentations

Students will complete at least four writing assignments or presentations as individuals and in small groups (2-3 people). These assignments will generally involve some analysis and/or comparison involving “real world” scenarios and application of general security controls (most frequently using OSU’s Security Framework as a common base for comparison). Each of the 4 projects will account for 15% of the total grade, for a total of 60% of the grade.

Discussions/Participation

Students are expected to discuss the weekly readings and “current events” in class and on-line. Grading will be based on relevance, accuracy of analysis and application of common security principles and controls. This will make up 30% of the grade.

Attendance

With certain exceptions (exams or exam reviews), I will take attendance every class period using Top Hat. Top Hat is online system whereby you use your phone, tablet or phone to acknowledge your class attendance. Days that attendance will be taken are noted with an "a" on the course schedule. *You may miss up to TWO classes without a loss of attendance points. After that, you will lose FIVE points for every class (noted with an "a" on the course schedule) that you miss.* See course policies below for more specific information. Attendance will be 10% of the total grade.

Grading Scale

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

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. Attendance will be taken every day, except where noted on the syllabus (e.g., exam and review days).

You must let me 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

I expect 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 me 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, I do understand that situations occasionally come up. I'm generally not concerned if an assignment is a few hours late, but if your assignment is more than a day late I will grade it for full credit only in situations where (1) the assignment was late due to unavoidable circumstances and (2) you let me know about your situation within 48 hours of missing the deadline. If you do not turn something in and you don't communicate with me within 48 hours of missing the deadline, you will receive zero points.

Grade Disputes

I am happy to revisit grades and to discuss my 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 are unsure, please give credit to your source or talk to me 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

It is the responsibility of the Committee on Academic Misconduct to investigate or establish procedures for the investigation of all reported cases of student academic misconduct. The term "academic misconduct" includes all forms of student academic misconduct wherever committed; illustrated by, but not limited to, cases of plagiarism and dishonest practices in connection with examinations. Instructors shall report all instances of alleged academic misconduct to the committee (Faculty Rule 3335-5-487). For additional information, see the Code of Student Conduct (http://studentaffairs.osu.edu/info_for_students/csc.asp).

Disability Statement

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

This schedule includes a tentative list of topics, readings and assignment due dates. In addition, I have created a module for each class (by date and topic) in Canvas. The class module contains more detailed information about the topic, readings, activities and reflection assignments. Failure to review a class module may result in you missing a reflection assignment or reading, which could negatively influence your discussion participation score.

Topic	week	day	Topics	Reading	Assignment
Course Overview	1	1	Course Overview; syllabus review; beyond the CIA triad; privacy, anonymity, attribution, repudiation	<p>"Beyond the CIA Triad", Jim West (https://isc2usmg.org/images/documents/Beyond_the_CIA_Triad.pdf)</p> <p>"Dilemas of the Internet Age: Privacy vs Security", Deena Zaru (http://www.cnn.com/2015/02/04/politics/deena-zaru-internet-privacy-security-al-franken/index.html)</p>	Discussion: Privacy and security: how do you define these? What's the relationship between the two?
Course Overview	1	2	Concepts and Terminology	<p>"An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants", Paxson et al (http://www.icir.org/vern/papers/miscreant-wealth.ccs07.pdf)</p> <p>"Show Me the Money: Characterizing Spame Advertised Revenue" (http://www.icir.org/vern/papers/ppair-usesec11.pdf)</p>	Discussion: Find an example of something security related being shared or sold on the Internet, share it with the class.
Tools for Thinking About Security	2	1	Attack trees, attack graphs	<p>Attack Trees, Shneier (https://www.schneier.com/academic/archives/1999/12/attack_trees.html)</p> <p>Attack Graphs (https://blogs.technet.microsoft.com/johnla/2015/04/26/defenders-think-in-lists-attackers-think-in-graphs-as-long-as-this-is-true-attackers-win/)</p>	Discussion: What costs are associated with risks and the security controls we use to address them?

Risk	2	2	Overview of Risk	Sample risk assessment, risk assessment template.(OSU)	Writing: create an attack tree; create an attack graph for attacks against cookies in a setting of your choosing.
OSU's Security Policies and Framework	3	1	Security policies and standards	Responsible Use: https://it.osu.edu/sites/default/files/files-1477502439/responsible-use-of-university-computing-and-network-resources-policy.pdf Data Classification: https://it.osu.edu/sites/default/files/files-1477502242/institutionaldata.pdf Data Elements: https://cybersecurity.osu.edu/system/files/2017/08/30/osuidp-dataelementclassificationassignments.pdf IT Security: https://it.osu.edu/sites/default/files/files-1477502296/itsecurity.pdf	None: focus on the reading for this week.
OSU's Security Policies and Framework	3	2	Information Security Standards	Information Security Standard: https://cybersecurity.osu.edu/system/files/osu.iss.v1.5.pdf Information Security Control Requirements (ISCR): https://cybersecurity.osu.edu/system/files/osu.iscr.v1.5.1.pdf	Writing: classify a given list of data, and for each list the services where it can be stored.
OSU's Security Policies and Framework	4	1	Information Security Standards	ISCR IT1-IT9, selected sample evidence of implementation	None: focus on the reading for this week.
OSU's Security Policies and Framework	4	2	Information Security Standards	ISCR IT10-IT18, selected sample evidence of implementation	Discuss: Thoughts on the OSU policies and standards? What is missing? What would you remove? Is there a better approach? How might you go about answering these questions if you don't know?
System Security	5	1	System hardening: CIS and related benchmarks, guides	CIS documentation, especially their Benchmarks. https://www.cisecurity.org/ Sample CIS scan of a Windows desktop	None: focus on the reading for this week.
System Security	5	2	System hardening: CIS and related benchmarks, guides	Review the benchmark spending assignment, discussion of how benchmarks are typically applied and managed.	Writing: Review a sample benchmark report, decide where to spend fake money to address the remaining issues, and get scored against revealed threats.

System Security	6	1	Malware case studies	<p>Understanding the Mirai Botnet (https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf)</p> <p>Lenovo (https://www.sans.org/reading-room/whitepapers/casestudies/lenovo-terrible-horrible-good-bad-week-35965)</p>	Discussion: Do some research, discuss an example of malware, why you found it interesting, what vulnerabilities (if any) were associated with it.
System Security	6	2	Anti-malware, host-based IDS, related topics	<p>Next Gen Security Software: Myths and Marketing (https://www.welivesecurity.com/2017/02/13/next-gen-security-software-myths-marketing/)</p>	Writing: Research ransomWare, write a brief summary of why its a problem now (as opposed to 10 years ago), what mitigations help prevent/handle it, etc.
System Security	7	1	Vulnerabilities, scanning, management CVSS, CVE	<p>Common Vulnerabilities and Exploits (CVE, https://cve.mitre.org/)</p> <p>Common Vulnerability Scoring System (CVSS, https://www.first.org/cvss/)</p>	Writing: assess the risk of several fictional vulnerabilities (to be provided), including justification for the values chosen. How would this guide your response to software exploiting that vulnerability?
System Security	7	2	Vulnerability case studies	<p>Everything You Know About the Vulnerabilities Equities Market is Wrong (Everything You Know About the Vulnerability Equities Process Is ...)</p> <p>Zero Days, Thousands of Nights... (Zero Days, Thousands of Nights: The Life and ... - RAND Corporation)</p> <p>For Good Measure: To Burn or Not To Burn (https://www.usenix.org/publications/login/summer2017/geer)</p>	Discuss: reflect on the readings - should the US expose or hide known vulnerabilities? Can you find other relevant material on this question?
System Security	8	1	Patch management; Asset management; Configuration management; Change management; File Integrity Management		Discussion: Between keystroke logging, session hijacking, password guessing, phishing: which presents the greatest risk to modern systems? How do you protect against this? Are there other authentication related threats?

Identity and Access Management	8	2	Review and discussion of elements of Identity Management through a role playing exercise (exploring authentication, authorization, accountability, single sign-on, multi-factor, password management, access management, and privileged account management).	Designing an Authentication System: A Dialogue in Four Scenes (http://web.mit.edu/kerberos/dialogue.html)	Writing: reflections on the in-class "game"
Threats	9	1	Threats, Threat Agents	The Landscape of Internet Threats (http://www.icir.org/vern/talks/ThreatLandscape.Brazil.May15.pdf) Recent CrowdStrike (or other) threat reports. The 2013 report was especially interesting to me.	Discussion: why might someone want to "attack" OSU's assets (systems, data, accounts...)? How important is that we enumerate/understand *all* of these? What's the difference between defending against nation-state attackers and other threats, such as hacktivists or spammers?
Threats	9	2	Nation-state threats	Stuxnet: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ Stuxnet: Zero Days (the movie) (optional) Kaspersky: https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html	None: focus on the reading or watch the movie.
Threats	10	1	Insider Threat, User Behavior Analytics	FBI's Counterintelligence Vulnerability Assessment for Academia CERT Insider Threat readings (https://www.cert.org/insider-threat/)	Writing: reflect on Inside Threats. What's easy/hard about preventing and detecting these? What's the relationship between an Inside Threat program and privacy?

Attacks, Intrusions, Intrusion Detection/Incident Response/Forensics	10	2	Kill chains; Tactics, Techniques and Procedures;	Lockheed Martin "Kill Chain" (https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf) Anything on TTP	Writing: Discuss mitigations for three attack patterns (to be provided)
Attacks, Intrusions, Intrusion Detection/Incident Response/Forensics	11	1	Security incident and data breach case studies.	Case studies on security incidents (SONY, Target, Home Depot, Equifax)	Discuss: find other case studies (preferably not mentioned by others),
Attacks, Intrusions, Intrusion Detection/Incident Response/Forensics	11	2	Intrusion Detection, Incident Response and Hunting (with a tabletop exercise)	Intrusion Detection and Incident Response prep reading	Writing: Intrusion Detection and Incident Response Tabletop post-mortem
Attacks, Intrusions, Intrusion Detection/Incident Response/Forensics	12	1	Penetration Testing: Red, Blue and Purple Teams	Sample pen-test scope document, template and report.	Discuss: what are the benefits and short-comings of penetration testing? How can the Red and Blue teams help each other improve?
Industrial Control Systems (ICS)	12	2	Industrial Control Systems, PERA Model	PERA web site (http://www.pera.net/) Current ICS related incidents	Discussion: what's the worst that could happen?
Cloud	13	1	Cloud services and the challenges we face in securing them - assessments and auditing, authentication, monitoring, investigations...	Cloud Security Alliance Guide (https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/CSAguide.v3.0.pdf) Romig: Security Operations Perspective on Cloud Services	Writing: in light of everything discussed so far, where are the challenges in adopting cloud solutions? What Cloud Services are in use at OSU? Any special challenges to the secure use of these services?
Internet of Things	13	2	The challenge of securing the Internet of Things.	Zigbee Exploited (https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf) DolphinAttack: Inaudible Voice Commands (https://arxiv.org/abs/1708.09537) This Doll May Be Recording What Children Say, Privacy Groups Charge (https://www.npr.org/sections/alltechconsidered/2016/12/20/506208146/this-doll-may-be-recording-what-children-say-privacy-groups-charge)	Discussion: In light of what we've discussed this semester and what you know about the Internet of Things, discuss what security controls should be applied to secure the IoT and what new controls might be needed.

Trends, the future, roadmaps	14	1	The past and future of Information Security, with particular attention to what's changing and what's not and how well we can predict future trends.	Verizon data breach report 2009, plus the current Verizon data breach report	Writing: pick two annual reports from the same source, three years apart (preferably one recent, one from three years ago). For the predictions made in the older report, which have come true, which haven't? Reflect on this and the ramifications for making plans for future security needs.
Summing up, loose ends	14	2	TBD		Writing: reflect on the main things you learned from this class (2-3 pages).

The Ohio State University
College of Arts and Sciences

Information Security Minor (INFOSEC-MN)

International Studies, 33 Townshend Hall, 1885 Neil Ave., Columbus, OH 43210-1222
614-292-9657; <http://internationalstudies.osu.edu>

Information security is the study of the dynamic interaction between the nature of cyber threats to the security, integrity and availability of information and the diverse efforts that are made to counter them.

The information security minor gives students a multidisciplinary perspective on the sources of, and reasons for, cyber threats and the strategies undertaken to counter them, including the role of computers and computing as well as that of laws, regulations and information storage standards and practices. Students are also introduced to successes and failures in protecting information against cyber attack through the detailed analysis of real-world case studies as well to the broader social, economic and security context in which cyber threats arise.

The information security minor requires 16 hours of academic credit.

**Some courses in this minor have pre-requisites. Please consult the course bulletin before enrolling in courses.*

Required Courses: (10 hours)

Computer Science and Engineering 2501
International Studies 3702
Computer Science and Engineering 4471
International Studies 4702

Critical Perspectives: choose two (6 credit hours minimum)

Communication 3332
Computer Science and Engineering 5351
Computer Science and Engineering 5473
International Studies 3700
International Studies 3701
International Studies 5191
Linguistics 3801
Linguistics 3802
Public Affairs 4000
Sociology 5525

Information Security minor program guidelines

Required for graduation No

Credit hours required A minimum of 16 credit hrs. 1000 level courses shall not be counted in the minor. At least 6 credits must be at the 3000 level or above.

Transfer and EM credit hours allowed

A student is permitted to count up to 6 total hours of transfer credit and/or credit by examination.

Overlap with the GE

A student is permitted to overlap up to 6 credit hours between the GE and the minor.

Overlap with the major and additional minor(s)

- The minor must be in a different subject than the major.
- The minor must contain a minimum of 12 hours distinct from the major and/or additional minor(s).

Grades required

- Minimum C- for a course to be listed on the minor.
- Minimum 2.00 cumulative point-hour ratio required for the minor.
- Course work graded Pass/Non-Pass cannot count on the minor.
- No more than 3 credit hours of coursework graded Satisfactory/Unsatisfactory may count toward the minor.

X193 credits No more than 3 credit hours.

Minor approval The minor must be approved by the academic unit offering the minor.

Filing the minor program form The minor program form must be filed at least by the time the graduation application is submitted to your college office.

Changing the minor Once the minor program is filed in the college office, any changes must be approved by the academic unit offering the minor.

College of Arts and Sciences
Curriculum and Assessment Services
154 Denney Hall, 164 W. 17th Ave.
<http://artsandsciences.osu.edu>

Concurrences for Information Security Minor

Sample Request

Claudia,

International Studies is proposing a new minor in Information Security and a Sociology course, Global Criminology, is included in the list of electives. A copy of the proposal is attached. With this note, I am requesting both your approval of the inclusion of this course and your support for the minor in general. Do get back to me if you have questions. Thanks.

Tony

Anthony Mughan
Professor, Political Science &
Director, International Studies
2140 Derby Hall
The Ohio State University
Columbus, OH 43210

Computer Science and Engineering

The Department of Computer Science and Engineering approves the inclusion of the following courses in International Studies' proposed Information Security minor:

CSE 2501: Social, Ethical and Professional Issues in Computing
CSE 4471: Information Security
CSE 5351: Introduction to Cryptography
CSE 5473: Network Security

The CSE Department also approves of the minor in general.

- Rephael Wenger

CSE Associate Chair

Rephael Wenger, CSE Associate Chair and Associate Professor
The Ohio State U., Dept. of Comp. Sci. and Eng.
485 Dreese Lab, 2015 Neil Ave, Columbus, Ohio 43210-1277
Tel: (614) 292-6253. E-mail: wenger.4@osu.edu

Sociology

Hi Tony

As Director of Undergraduate Studies for the Department of Sociology, I give approval for the inclusion of the Global Criminology course in this minor and support the minor in general, it sounds like it will be very useful for our students!

Best

Andrew

Andrew W. Martin

Professor and Director of Undergraduate Studies

Department of Sociology

238 Townshend Hall,

1885 Neil Avenue, Columbus, OH 43210

614-247-6641 Office

martin.1026@osu.edu

Linguistics

Hi Tony,

I have circulated the concurrence to our faculty, and they are quite supportive. The new minor looks interesting, and we are happy to support both the inclusion of the course and the minor.

Our undergraduate program coordinator, Julie McGory, cc:d here, had this comment:

Perhaps it would be a good idea to add Ling3802, Language and Computers to the electives? That course, now 3802, is in the process of being changed to 2801. There are no 2000 level courses in the electives, and perhaps having 2801 might make the minor more appealing/accessible to some students. I realize there might be curricular reasons why Language and Computers may not fit into the minor electives, but wanted to at least raise the question.

Best,

Shari

--

Shari R Speer, PhD

Professor

Chair of Department

College of Arts and Sciences Department of Linguistics

until 10/30/17:

108B Stadium East, 1961 Tuttle Park Place, Columbus, OH 43210-1234

as of 10/30/17

101A Oxley Hall

1712 Neil Ave, Columbus, OH 43210-1234

Shari,

Thanks to you and Julie for pointing out the relevance of Ling. 3802: Language and Computers. We have decided to add it to the list of electives. Could you send me a very brief addendum signalling your agreement to list this course as well. Sorry!

Tony

Yes, I am happy to support your inclusion of 3802.

Best,

Shari

Shari R. Speer

Professor

Chair of Department

The Ohio State University College of Arts and Sciences Department of Linguistics

108B Ohio Stadium East, 1961 Tuttle Park Place, Columbus, OH 43210

614.292.5389 Office

John Glenn College

Hi Tony,

The Glenn College is happy to offer concurrence for the proposed new minor in Information Security.

Thank you for including our Public Affairs 4000 Public Policy Evaluation class as one of the electives.
Rob

Robert T. Greenbaum

Professor, Associate Dean for Curriculum

John Glenn College of Public Affairs

350E Page Hall, 1810 College Road, Columbus, OH 43210

614-292-9578 Office / 614-292-2548 Fax

Communication

We think this sounds to be an interesting and timely minor, on a topic that is likely only to increase in societal relevance, and will be glad to see our course Communication 3332: Risk Communication (3 credit hours) listed. Note there is no "s" on the word Communication on the course identification.

Best,

Mike

Michael D. Slater

Director

Social and Behavioral Sciences Distinguished Professor

School of Communication

3016 Derby Hall, 154 N. Oval Mall

The Ohio State University

Columbus, OH 43210

Slater.59@osu.edu

Phone: 614-292-3400