Cybersecurity Foundations:
An Interdisciplinary Introduction

Name: Dr. West Brown
Email: wbrown@css.edu
Phone: (000)-000-0000
Office Number: Mumford Hall – 208C
Office Hours: TR 14:00 – 16:00 (in-person), W 13:00-15:00 (virtual)

Term: Fall 2012
Meeting Days: Tuesday, Thursday
Meeting Time: 12:00 – 13:30
Class Location: Twinn Hall – 306
Credits: 3

I. Course Overview

Cybersecurity is a dynamic and growing industry. As an academic discipline, cybersecurity has never been deeper or more important, having evolved from a relatively obscure concentration into a highly complex, interdisciplinary field rich in both research possibilities and real-world applications.

As the world enters an age increasingly defined by information technology systems, we find ourselves increasingly reliant upon computer-based technologies. As this reliance on computers grows stronger in all aspects of modern life, so too do attacks on computers and networks. It therefore becomes increasingly necessary – and increasingly challenging – to secure the technological tools that play a critical role in our personal and professional lives.

Cyber threats against individuals, governments, and businesses are continually taking on newer, more complex, and more dangerous forms. At this moment, highly skilled cyber attackers around the world are in the process of crafting revolutionary attack methods to thwart the latest cybersecurity innovations. As a consequence, cybersecurity professionals today must possess a range of academic and technical skills to secure information and infrastructure and combat new attacks.

The purpose of this course is to provide an introduction to the range of disciplines that are fundamental to protecting cyber assets in the modern world. Students will learn what cybersecurity is, how it has evolved since the 1940s, and how cybersecurity frameworks can be applied across a wide range of contexts and industries. This course will also provide an introduction to the various technical and non-technical skills that are foundational in any cybersecurity career. During this course, students will gain the professional and academic foundations to pursue further study and concentration in any aspect of cybersecurity.

II. Prerequisites

There are no prerequisites for this course

III. Course Topics

- Introduction to Cybersecurity
- Risk Management
- Cybersecurity Law, Policy, and Analysis
- Management Theory and Practice
- Fundamentals of Computer Science
- Private Sector Applications of Cybersecurity
- Cybersecurity Research and Methods

IV. Learning Objectives

1. Gain an appreciation and basic understanding of the key disciplines that support cybersecurity capabilities, including computer science, risk management, program management, and federal law and policy
2. Understand the depth and breadth of cyber-based threats in the modern world
3. Become familiar with key national and global institutions and their influence on international cybersecurity policies and standards
4. Understand the structure and functions of the U.S. federal government with regard to national cybersecurity
5. Learn the obligations of private sector companies with regard to information security
6. Recognize the government-mandated initiative to leverage both public and private sector cybersecurity capabilities in order to respond to growing physical and computer-based threats against U.S. critical infrastucture
7. Gain basic fluency in the quantitative disciplines that support advanced cyber security practice, including risk quantification, management sciences, Earned Value Management, and cost-benefit analyses
8. Understand the theory and practice of risk management, as well as ways to assess and mitigate risk
9. Become familiar with key computer science and engineering concepts that inform cybersecurity capabilities, including programming, hardware and software, and IT architecture
10. Learn common methods of cyber attacks and exploits, and some of the ways that organizations have learned to anticipate and protect themselves from these threats

11. Understand how to plan and execute cybersecurity programs, and how this process is conducted at the federal level
12. Gain a deep appreciation for cybersecurity research, including ways to research the evolving cybersecurity laws and policies of the U.S. federal government

V. Required Text

Lee Zeichner, Cybersecurity Foundations: An Interdisciplinary Introduction, ZRA ©2012

VI. Course Requirements

Homework: Each week, students will receive a set of practice problems. These problems will be due at the beginning of class each Tuesday and will be graded for completion. Late assignments will receive 25% credit.

Quizzes: There will be a weekly quiz. These quizzes will cover any material mentioned in class or within the textbook chapter assigned for the week.

Team Project: During the middle of the semester, students be required to complete a case study project. Each group of five students will have three project topics to choose from. Each group will be required to complete ONE 7-page paper, create a slide show, and give a 20-minute presentation. This project will be DUE AT THE BEGINNING OF CLASS **OCTOBER 11TH**.

Term Paper: One 8-page term paper will be DUE AT THE BEGINNING OF CLASS **NOVEMBER 27TH**. A list of topics and additional information about the term paper will be available in-class on the date listed within the course schedule below. NO LATE PAPERS WILL BE ACCEPTED.

Final Exam: At the end of the semester, each student will be responsible for completing a 2-hour final exam. The exam will be comprehensive, including all of the information covered throughout the semester.

VII. Grading System

Course Item	Percent of Final Grade
Homework	5%
Quizzes	10%
Team Project	20%
Term Paper	25%

Final Exam	40%
Total	**100%**

VIII. Office Hours

Virtual office hours will take place each Wednesday from 13:00 – 15:00. I will also be available TR from 14:00 – 16:00 for in-person office hours in my office, Mumford Hall – 208C

IX. Course Schedule

Week 1: Introduction to Cybersecurity

This week, we will define cybersecurity as a field and explore how cybersecurity challenges have unfolded in the past seventy years. We will learn the fundamental areas of knowledge that professionals need to master in order to solve modern cybersecurity problems.		
Read Before Class	Day 2	• National Security Decision Directive-145 • Sanger, David E. "Chapter 10: The Dark Side of the Light Footprint." *In Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Crown Publishers, 2012. 243-273. • Zeichner, Lee. "Introduction: From ARPANET to Stuxnet." In *Cybersecurity Foundations: An Interdisciplinary Introduction*.
Cover In Class	Day 1	• Syllabus overview • Interdisciplinary nature and importance of cybersecurity
	Day 2	• Cybersecurity principles and challenges

Week 2: Risk Management for Cybersecurity: Overview

This week, we will discuss Risk Management for cybersecurity, and learn about Threat and Vulnerability Assessments		
Read Before Class	Day 1	• National Energy Regulatory Commission (NERC). "Cyber Attack Task Force: Final Report." May 9, 2012. pp. 1-10. http://www.nerc.com/docs/cip/catf/12-CATF_Final_Report_BOT_clean_Mar_26_2012-Board%20Accepted%200521.pdf • U.S. Department of Energy. "Electricity Subsector Cybersecurity Risk Management Process 2012." http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf • Zeichner, Lee. "Chapter 1: Risk Management for Cybersecurity." In *Cybersecurity Foundations: An Interdisciplinary Introduction*.
	Day 2	• Department of Homeland Security, National Infrastructure Protection Plan (NIPP) Risk Management Framework (2009) • Department of Homeland Security, Risk Lexicon (September 2010) • National Institute of Standards and Technology (NIST), NIST SP 800-53, Recommended Security Controls for Federal Information Systems (August 2009) • National Institute of Standards and Technology (NIST), NIST SP 800-39, Managing Information Security Risk (March 2011)
Cover In Class	Day 1	• Introduction to risk management for cybersecurity • Interactive case study, protecting a home
	Day 2	• Threat assessments and vulnerability assessments

Week 3: Risk Management for Cybersecurity: Consequence and Risk Determination

This week, we will cover Consequence Assessments and Risk Determination, and quantitative and graphical risk determination models.		
Read Before Class	Day 1	• Department of Homeland Security, National Infrastructure Protection Plan (NIPP) Risk Management Framework (2009) • Department of Homeland Security, Risk Lexicon (September 2010)
	Day 2	• U.S. Department of Energy. "Electricity Subsector Cybersecurity Risk Management Process 2012." http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf
Cover In Class	Day 1	• Consequence assessment and risk determination
	Day 2	• Quantitative and graphical risk determination models

Week 4: Risk Management for Cybersecurity: Risk Response and Monitoring

This week, we will cover Risk Response and Monitoring techniques.		
Read Before Class	Day 1	• Zeichner, Lee. "Chapter 1: Risk Management for Cybersecurity." In *Cybersecurity Foundations: An Interdisciplinary Introduction*.
	Day 2	• Risk management Tabletop Worksheet
Cover In Class	Day 1	• Risk response and monitoring techniques
	Day 2	• Risk management Tabletop exercise

Week 5: Cybersecurity Law and Policy:
Introduction to Cybersecurity and the Federal Government

This week, we will introduce fundamental cybersecurity concepts regarding law and policy. We will learn the history of cybersecurity and its development as a national and global policy challenge. We will study the roles and responsibilities of the President and Congress in producing cybersecurity laws and policies, and critically examine the information security laws and policies of the United States government since 1965.

Read Before Class	Day 1	• Brooks Act CRS Summary • Computer Security Act CRS Summary • NSDD 145 • Sharp Sr., Walter Gary. “The Past, Present, and Future of Cybersecurity.” Journal of National Security Law & Policy vol. 4, no. 1 (2010): 13-26. http://jnslp.com/wp-content/uploads/2010/08/03_Sharp.pdf • Warner Amendment • Zeichner, Lee. “Chapter 2: Cybersecurity Law and Policy.” In *Cybersecurity Foundations: An Interdisciplinary Introduction*.
	Day 2	• Clinger-Cohen Act CRS Summary • Executive Order 13011 • Memoranda 97-02 • OMB Circular No. A-130 • Paperwork Reduction Act CRS Summary
Cover In Class	Day 1	• Cybersecurity and the federal government
	Day 2	• Civilian versus military control of federal information systems

Week 6: Cybersecurity Law and Policy: Development of Modern Cybersecurity Policy

This week, we will discuss the development of modern cybersecurity policy and the state of contemporary cybersecurity policy.

Read Before Class	Day 1	• Executive Order 13228 • Executive Order 13231 • Federal Information Security Management Act (FISMA) CRS Summary • Homeland Security Act (HSA) of 2002 CRS Summary • Homeland Security Presidential Directive 7 (HSPD-7) • NSPD-54/HSPD-23 • Presidential Decision Directive 63 (PDD-63)
	Day 2	• Cyberspace Policy Review, White House, 2009 http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf • Department of Homeland Security. “Blueprint for a Secure Cyber Future.” November 2011. http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf • Dycus, Stephen. "Congress's Role In Cyber Warfare." Journal of National Security Law & Policy vol. 4, no. 1 (2010): 155-171. http://jnslp.com/wp-content/uploads/2010/08/11_Dycus.pdf
Cover In Class	Day 1	• Modern cybersecurity policy
	Day 2	• Contemporary and future cybersecurity policy

Week 7: Fundamentals of Management for Cybersecurity: Introduction

This week, we will establish a clear distinction between managerial and technical work. We will see how management skills apply to cyber problems, and we will study and critically examine the formal managerial framework used in federal government cybersecurity programs.

Read Before Class	Day 1	• Schwalbe, Kathy. “Chapter 1: Introduction to Project Management” and “Chapter 2: The Project Management and Information Technology Context.” In Information Technology Project Management. • Zeichner, Lee. “Chapter 3: Fundamentals of Management for Cybersecurity.” In *Cybersecurity Foundations: An Interdisciplinary Introduction*.
	Day 2	• National Response Framework Summary • National Strategy to Secure Cyberspace Summary • NIST. “Frequently Asked Questions: Continuous Monitoring.” June 2010. http://csrc.nist.gov/groups/SMA/fisma/documents/faq-continuous-monitoring.pdf
Cover In Class	Day 1	• What do managers do?
	Day 2	• US-CERT case study

Week 9: Fundamentals of Management for Cybersecurity: Government Tools and Frameworks

This week, students will be introduced to the many complexities and challenges of program management. Students will learn how the Department of Homeland Security (DHS) plans and manages its cybersecurity programs. Students will read real-world examples of project management processes in order to connect theory and practice.

Read Before Class	Day 1	• "Chapter 1.2: Planning, Programming, Budgeting and Execution (PPBE) Process" in Defense Acquisition Guidebook https://acc.dau.mil/CommunityBrowser.aspx?id=488289#1.2 • (Sample CONOPS) Federal Interagency Geospatial Concept of Operations. http://www.nsgic.org/public_resources/DHS_Geospatial_CONOPS_v30_85x11.pdf • (Sample DHS CONOPS) DHS Interaction With State and Local Fusion Centers Concept of Operations http://www.fas.org/irp/agency/dhs/conops.pdf • (Sample DHS MNS Template) TSA Mission Need Statement Guide http://www.tsa.gov/video/pdfs/mds/TSAMNSGuide%28042607%29.pdf • (Sample DHS MNS) Integrated Deepwater System Mission Needs Statement http://www.uscg.mil/history/docs/2004_USCG_revisedmns.pdf • DoD PPBE An Executive Primer https://www.documentcloud.org/documents/293931-dodarmyppbeprimernov-2011.html
Cover In Class	Day 1	• Managerial challenges & the DHS Managerial Framework
	Day 2	• The DHS Managerial Framework: Theory and Practice

Week 10: Computer Science Fundamentals and Cybersecurity Operations

Students will learn the basic structure of computers and IT tools, as well as the various languages and processes that are fundamental to the efficient transfer of information via the Internet. Students will be introduced to the various attack methods that threaten information in cyberspace, as well as the processes and tools organizations use to protect themselves and their information from cyber attacks.		
Read Before Class	Day 1	• Zeichner, Lee. "Chapter 4: Computer Science Fundamentals and Cybersecurity Operations." In *Cybersecurity Foundations: An Interdisciplinary Introduction*.
	Day 2	• Maps, diagrams, and illustrated facts about the Internet: http://mountpeaks.wordpress.com/2012/03/06/what-has-the-internet-evolved-into-nowadays/ • Commercial Communications Satellite map http://comsoft-sat.com/app/download/5782687752/Commercial+Communications+Satellites.png • Internet History Timeline: http://www.computerhistory.org/internet_history/
Cover In Class	Day 1	• Computing and information technology fundamentals
	Day 2	• The Internet

Week 11: Computer Science Fundamentals and Cybersecurity Operations: Cyber Attacks and Cybersecurity Operations

Students will be able to identify the characteristics of cyber attacks and exploits, and learn technical ways to anticipate and defend against them.

Read Before Class	Day 1	• Frontline: Cyberwar Interactive Website http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/ • ICS-CERT. "Incident Response Summary Report 2009-2011." https://ics-cert.us-cert.gov/sites/default/files/documents/ICS-CERT%20Incident%20Response%20Summary%20Report%20%282009-2011%29_accessible.pdf • NIAC Prioritizing Cyber Vulnerabilities 2004. http://www.dhs.gov/xlibrary/assets/niac/NIAC_CyberVulnerabilitiesPaper_Feb05.pdf • Zeichner, Lee. "Chapter 4: Computer Science Fundamentals and Cybersecurity Operations." In *Cybersecurity Foundations: An Interdisciplinary Introduction.*
	Day 2	• An Annex to the NIPP: Communications Sector-Specific Plan 2010. http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf • FERC Example Security Plan http://www.ferc.gov/industries/hydropower/safety/guidelines/security/security-plan-example.pdf • NIST SP 800-64 http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf • The DHS Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure. http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg72229/pdf/CHRG-112hhrg72229.pdf
Cover In Class	Day 1	• Cyber attacks and exploits
	Day 2	• Cybersecurity operations

Week 12: Cybersecurity for the Private Sector

We will introduce fundamental private sector concepts and principles. Students will learn basic legal and regulatory challenges facing the private sector, including legal liability. Students will be able to identify, explain, and analyze major legal and regulatory rules that the private sector must address as a routine part of cybersecurity planning. We will outline models for robust cybersecurity plans and programs for the private sector.

Read Before Class	Day 1	• Zeichner, Lee. “Chapter 5:Cybersecurity for the Private Sector.” In *Cybersecurity Foundations: An Interdisciplinary Introduction*. • Management’s Role in Information Security in a Cyber Economy http://irps.ucsd.edu/assets/001/501280.pdf
	Day 2	• Cyber Security Incident Reporting and Response Planning 008-04 (CIP-008-04) • FTCA violation against TJX • Gramm-Leach-Bliley Financial Modernization Act CRS Summary http://thomas.loc.gov/cgi-bin/bdquery/z?d106:SN00900:@@@D&summ2=m& • Health Information Technology for Economic and Clinical Health Act (HITECH) CRS Summary (American Recovery and Reinvestment Act of 2009, Title XIII) http://thomas.loc.gov/cgi-bin/bdquery/z?d111:HR00001:@@@D&summ2=m& • Health Insurance Portability and Accountability Act (HIPAA) CRS Summary http://thomas.loc.gov/cgi-bin/bdquery/z?d104:HR03103:@@@D&summ2=m& • Sarbanes-Oxley Act (SOX) CRS Summary http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR03763:@@@D&summ2=m&
Cover In Class	Day 1	• What is a corporation? • The legal obligations of corporations
	Day 2	• Cybersecurity legislation and the private sector

Week 13: Cybersecurity for the Private Sector:
Methods of Protecting Private Sector Networks

Students will learn the many ways in which leaders of private sector companies think, plan, and act in order to protect their IT systems.		
Read Before Class	Day 1	• Allen, Julia H. Governing for Enterprise Security Implementation Guide. “Article 1: Characteristics of Effective Security Governance.” Carnegie Mellon University, Software Engineering Institute. http://www.cert.org/governance/ges.html • Dunn, Catherine. Boards of Directors Largely Ignoring Corporate Cyber-Risk Management http://www.law.com/jsp/cc/PubArticleCC.jsp?id=1202544750336&Boards_of_Directors_Largely_Ignoring_Corporate_CyberRisk_Management • FEMA Business Continuity Plan website http://www.ready.gov/business/implementation/continuity • Jain, Raj. Intrusion Detection Systems http://www1.cse.wustl.edu/~jain/cse571-07/ftp/l_23ids.pdf • Kundra, Vivek. “25 Point Implementation Plan to Reform Federal Information Technology Management,” Dec. 9, 2010. http://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf • Sample Business Continuity Plan (worksheet) http://www.ready.gov/sites/default/files/documents/files/BusinessContinuityPlan.pdf
Cover In Class	Day 1	• The model cybersecurity plan for the private sector

Week 14: Cybersecurity for the Private Sector: Methods of Protecting Private Sector Networks

Students will learn some of the "big picture" complications associated with implementing cybersecurity measures in the private sector. Students will gain insight into the connections between cybersecurity and sound business practices. Students will understand the legal and financial consequences of neglecting cybersecurity. Moving into Chapter 6.0, students will learn how federal rules and regulations are created and how cyber crimes are prosecuted, and gain a foundation of knowledge for performing research in the field.		
Read Before Class	Day 1	• FTC Complaint Against TJX http://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801tjxcomplaint.pdf • FTC Agreement with TJX http://www.ftc.gov/sites/default/files/documents/cases/2008/03/080327agreement_0.pdf • FTC Complaint Against Twitter http://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twittercmpt.pdf • FTC Agreement with Twitter http://www.ftc.gov/sites/default/files/documents/cases/2010/06/100624twitteragree.pdf • FTC Complaint Against Sony http://www.ftc.gov/sites/default/files/documents/cases/2008/12/081211cmp0823071.pdf • FTC Agreement with Sony http://www.ftc.gov/os/caselist/0823071/081211consentp0823071.pdf
	Day 2	• (Video) "Legislative Research" • Albert Gonzalez Case Study • Computer Fraud and Abuse Act (CFAA) CRS Summary http://thomas.loc.gov/cgi-bin/bdquery/z?d099:HR04718:@@@D&summ2=m& • Dove, Robert B. "Enactment of a Law." http://thomas.loc.gov/home/enactment/enactlaw.pdf • Sullivan, John V. "How Our Laws Are Made." 2007. http://www.gpo.gov/fdsys/pkg/CDOC-110hdoc49/pdf/CDOC-110hdoc49.pdf • Zeichner, Lee. "Chapter 6: Advanced Cybersecurity Studies." *Cybersecurity Foundations: An Interdisciplinary Introduction*.
Cover In Class	Day 1	• TJX, Twitter, and Sony Case Studies
	Day 2	• The roles of the President, Congress, and the courts in cybersecurity legislation, regulation, crime, and punishment

Week 15: Advanced Cybersecurity Studies

<table>
<tr><td colspan="3">Students will be able to identify major executive branch policy documents on cybersecurity and understand the role of the President in shaping cybersecurity policy. Students will further understand the interplay between the three branches of government regarding cybersecurity laws and policies. Students will understand the federal regulations process and be able to use and analyze the Federal Register.</td></tr>
<tr><td rowspan="2"><b>Read Before Class</b></td><td>Day 1</td><td>• (Video) “Executive Policy”
• (Video) House Committee on Homeland Security. “Subcommittee Hearing: Preventing Nuclear Terrorism: Does DHS have an Effective and Efficient Nuclear Detection Strategy?” http://homeland.house.gov/hearing/subcommittee-hearing-preventing-nuclear-terrorism-does-dhs-have-effective-and-efficient
• Bush, George W. HSPD-7. 2003
• Clinton, William J. PDD-63. 1998
• DHS strategy and business model
• Organization of the National Security Council Packet (PDD-1, NSPD-1, PPD-1, HSPD-1 clips)</td></tr>
<tr><td>Day 2</td><td>• “The Reg Map” http://www.reginfo.gov/public/reginfo/Regmap/regmap.pdf
• (Video) “Federal Regulations”
• DHS. The Comprehensive Cybersecurity Initiative. http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf</td></tr>
<tr><td rowspan="2"><b>Cover In Class</b></td><td>Day 1</td><td>• Executive Branch cybersecurity policy</td></tr>
<tr><td>Day 2</td><td>• Federal cybersecurity regulations and the rulemaking processes</td></tr>
</table>

Week 16: Advanced Cybersecurity Studies: Federal Cybersecurity Regulations & Global Cybersecurity Policy

This week we will discuss how the interactions between Congress and the President shape cybersecurity regulations.		
Read Before Class	Day 1	• Brunner, Elgin M. and Manuel Suter. International CIIP Handbook 2008/2009. pp 463-521 http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf • Davis, Joshua. Hackers Take Down the Most Wired Network in Europe. Wired Magazine, 2007. http://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all • Jacobs, Andrew and Miguel Helft. “Google, Citing Attack, Threatens to Exit China.” New York Times. January 12, 2010 http://www.nytimes.com/2010/01/13/world/asia/13beijing.html • Maurer, Tim. Cyber Norm Emergence at the United Nations. September 2011. http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf
	Day 2	• Review of Chapter 6 readings.
Cover In Class	Day 1	• Global cybersecurity institutions and policies
	Day 2	• Exam Review

Wk	Month	Tues	Thurs	Relevant Reading	Material Covered in Tuesday Lecture	Material Covered in Thursday Lecture
1	Aug.	28	30	Intro	Importance of Cybersecurity	Cybersecurity Principles and Challenges
2	Sept.	4	6	Ch. 1	Introduction to Risk Management	Threats and Vulnerabilities
3		11	13	Ch. 1	Consequences and Risk Determination	Quantitative Risk Determination Models
4		18	20	Ch. 1	Risk Response and Monitoring	Risk Management Tabletop Exercise
5		25	27	Ch. 2	Cybersecurity and the Federal Government	Civilian vs. military control of federal information systems
6	Oct.	2	4	Ch. 2	Development of Modern Cybersecurity Policy	Contemporary & Future Cybersecurity Policy
7		9	11	Ch. 3	Introduction to Management ("What do managers do?")	Continuous Monitoring Systems, US-CERT Case Study **(Team Project Due)**
8		**16**	**18**		**Fall Break**	**Fall Break**
9		23	25	Ch. 3	Managerial Challenges & the DHS Managerial Framework	The DHS Managerial Framework: Theory & Practice
10	Oct./ Nov.	30	1	Ch. 4	Computing and IT Fundamentals	The Internet
11		6	8	Ch. 4	Cyber Attacks & Exploits	Cybersecurity Operations
12		13	15	Ch. 5	What is a corporation?	Cybersecurity Legislation and the Private Sector
13		20	**22**	Ch. 5	The Model Cybersecurity Plan for the Private Sector	**Thanksgiving**
14		27	29	Ch. 6	Table Top Exercise – TJX, Twitter, Sony **(Term Paper Due)**	Congress and the Courts – Cyber Crime and Punishment
15	Dec.	4	6	Ch. 6	Executive Branch - Policy	Federal Cybersecurity Regulations
16		11	13	Ch. 6	Global Cybersecurity Institutions and Policies	Exam Review

Final Exam – Thursday December 20th @ 19:00-21:00 (7:00pm-9:00pm) Rooms TBA