Carnegie Mellon University
H. John Heinz III School of Public Policy and Management

Spring 2015 (W3)
(90-895) Policy Topics:
Cybersecurity Policy

Instructors
Earl Crane
crane@andrew.cmu.edu

Robert Novy
rnovy@andrew.cmu.edu

Time & Location
January 12, 2015 – March 2, 2015 (7 Sessions)
6:00 PM – 8:50 PM

Carnegie Mellon University
444 N. Capitol Street, NW Suite 399
Washington, D.C. 20001

Video Conference
None

Course Description
Cybersecurity impacts our daily lives and national security in ways previously never considered. The rapid increase in technology dependence has brought enormous economic benefits and societal improvements – but at the expense of increased opportunities to exploit that dependence for economic and political gain. President Obama has cited that the “cyber threat is one of the most serious economic and national security challenges we face as a nation” and that “America's economic prosperity in the 21st century will depend on cybersecurity.”

Public policy has struggled to keep pace with the rapid change of technology, from individual privacy and civil liberties to the resiliency of critical infrastructure. Too frequently public policy has been forced to play catch-up after a significant weakness is exposed or loss incurred to focus efforts to safeguard information, defend interconnected systems, deter online crime and protect human rights exposed through digital weaknesses.

This course will provide second year masters level students with the knowledge and background information necessary to effectively govern the security of both federal, critical infrastructure, and private-sector IT systems. This program will expose students to the historical context leading up to the modern public policy for information security, and the current issues and trends influencing today’s decision makers.
Course Objectives
At the end of this course, students should be able to:
- Define relevant topics within cybersecurity and their policy implications
- Identify major issues and players within cybersecurity
- Articulate the challenges and differences between various cybersecurity approaches, both domestically and internationally
- Be able to apply their learning to their current internship environment
- Extrapolate cybersecurity implications for future or predicted events
- Identify major cybersecurity threats and trends
- Intelligently describe a cybersecurity incident (a “hack”) and what it means
- Identify and describe major US cybersecurity organizations, government agencies, policies and issues
- Articulate why cybersecurity is important to national security
- Deliver a cybersecurity policy brief for senior decision makers

Academic Integrity
Plagiarism means using words, ideas, or arguments from another person or source without citation. Cite all sources consulted to any extent (including material from the internet), whether or not assigned and whether or not quoted directly. For quotations, four or more words used in sequence must be set off in quotation marks, with the source identified.

Any form of cheating will immediately earn you a failing grade for the entire course. By remaining enrolled, you consent to this policy. I will seek the harshest penalties under CMU’s policy on “Standards for Academic and Creative Life” and “Cheating and Plagiarism” in the Student Guidebook (aka The Word, online at http://www.studentaffairs.cmu.edu/theword/)

Biographical Background
Earl Crane, Ph.D.
Earl is a recognized expert in information security and cybersecurity strategy and policy. He is currently a consultant with Promontory Financial Group, specializing in helping clients develop strategic solutions to growing cybersecurity challenges.

As the director for federal cybersecurity policy on the president’s National Security Staff from 2011 to 2013, Earl led federal cybersecurity policy and oversight for the cybersecurity coordinator, and was responsible for aligning and responding to shifting cybersecurity threats and vulnerabilities throughout the federal executive branch. In July of 2013, the President personally highlighted his efforts leading to a more secure Federal Government. He coordinated with senior government leaders to provide direction and streamline processes in a number of disciplines, including continuous monitoring, strong authentication, cloud computing, mobile computing, FISMA compliance, incident response, and information sharing and safeguarding.
From 2005 to 2011, Earl worked for the Department of Homeland Security, where he was the director of cybersecurity strategy and the chief information security architect. He supervised staff creating and implementing the DHS security risk-management strategy, and led the development of enterprise wide security architecture, policies and procedures to address issues including intrusion detection and response, security operations, threat intelligence, cloud computing security, and data-loss prevention. His background bridges evolving concepts in academic information-security management and practical implementation requirements.

Prior to DHS, Earl was a senior security consultant at Foundstone Inc., a division of McAfee, where he led the risk and regulatory compliance consulting services, and managed risk assessments, security architecture, penetration testing, incident response, and computer and network forensic analysis.

Ph.D., engineering management, George Washington University
M.S., information security management, Carnegie Mellon University
B.S., mechanical engineering, Carnegie Mellon University

Robert Novy
Robert Novy has over 25 years of federal government experience and is currently with the Department of Homeland Security where he focuses on government and public affairs.

Previously, Robert Novy served as the Director for Cybersecurity Policy on detail to the National Security Staff. He was responsible for the formulation and execution of cybersecurity incident response, intelligence and defense policy for the White House.

Prior to this position, his other federal government assignments were in Washington DC and New York City.

Throughout his career, he initiated and managed high profile transnational cyber investigations encompassing network intrusions and the theft of data, information and intellectual property from financial institutions and government systems. He began his career investigating financial, electronic, and cyber crimes as well as conducting computer forensic examinations.

He has instructed and lectured extensively on the subjects of protection, critical infrastructure, digital forensics, investigations, and information security.

Prior to his DHS career, he also worked for the Department of Treasury, the U.S. Securities and Exchange Commission and also served in the U.S. Navy.

He graduated from Troy State University (now Troy University) with a Master of Public Administration and from the University of the State of New York, Regents College (now Excelsior College) with a Bachelor of Science.

Disclaimer from Professor Crane and Professor Novy
The views that are expressed are our own and not the position of our employers or the United States Government. Though recent disclosures have leaked classified documents into the public domain, this course will only cover unclassified information approved for release to the public.

Course Schedule
Hours: 6:00-8:50 PM Monday

<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week 1</td>
<td>12 January</td>
<td>Background and history of information security</td>
</tr>
<tr>
<td></td>
<td>19 January</td>
<td>No Class – Martin Luther King Day</td>
</tr>
<tr>
<td>Week 2</td>
<td>23 January</td>
<td>Overview of national security structure</td>
</tr>
<tr>
<td>Week 3</td>
<td>2 February</td>
<td>Current state of Cybersecurity</td>
</tr>
<tr>
<td>Week 4</td>
<td>9 February</td>
<td>Incident Response, Electronic Crimes, and Crisis Communications</td>
</tr>
<tr>
<td>Week 5</td>
<td>16 February</td>
<td>Enterprise Governance &amp; Strategic Planning</td>
</tr>
<tr>
<td>Week 6</td>
<td>23 February</td>
<td>Partnerships</td>
</tr>
<tr>
<td>Week 7</td>
<td>2 March</td>
<td>Cybersecurity Policy Exercise (Exam)</td>
</tr>
</tbody>
</table>

Course Minutiae

Grading Rubric

<table>
<thead>
<tr>
<th>Grade</th>
<th>Interpretation</th>
<th>Points</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>A+</td>
<td>Exceptional</td>
<td>4.33</td>
<td>97-100+</td>
</tr>
<tr>
<td>A</td>
<td>Excellent</td>
<td>4.00</td>
<td>93-96</td>
</tr>
<tr>
<td>A-</td>
<td>Very Good</td>
<td>3.67</td>
<td>90-92</td>
</tr>
<tr>
<td>B+</td>
<td>Good</td>
<td>3.33</td>
<td>87-89</td>
</tr>
<tr>
<td>B</td>
<td>Acceptable</td>
<td>3.00</td>
<td>83-86</td>
</tr>
<tr>
<td>B-</td>
<td>Fair</td>
<td>2.67</td>
<td>80-82</td>
</tr>
<tr>
<td>C+</td>
<td>Poor</td>
<td>2.33</td>
<td>77-79</td>
</tr>
<tr>
<td>C</td>
<td>Very Poor</td>
<td>2.00</td>
<td>73-76</td>
</tr>
<tr>
<td>C-</td>
<td>Minimal Passing</td>
<td>1.67</td>
<td>70-72</td>
</tr>
<tr>
<td>R</td>
<td>Failing</td>
<td>0.00</td>
<td>-70</td>
</tr>
</tbody>
</table>

Grading Criteria
Class Participation / Weekly Assignments: 50%
Cyber Policy Exercise Paper: 35%
Cyber Policy Exercise Presentation: 15%

Attendance Policy
Students should attend all classes and comment on other student postings on blackboard. Class participation each day and at least one posting each week account for 5% of your
overall grade. Absent students will not earn class participation for the days absent. However, there can be unforeseen circumstances and emergencies that arise. Students may be granted the opportunity to earn 5% extra credit to make up for an excused absence, such as an illness, personal emergency, or an apprenticeship-related travel/opportunity that is worked out with me in advance of the missed class. After the one excused absence, the student will not receive participation credit for any missed classes. This will factor into the student’s final grade for the course. The student should contact me to work out the topic for the extra credit paper. Please note that even if a student misses a class (whether excused or unexcused), assignments due for that day must still be completed and handed in. Under certain circumstances, such as illness of the student, the instructor may grant extensions to due dates.

Office Hours
Faculty will be available prior to and after class to talk to students or phone consultations can be requested by emailing/making arrangements with the faculty directly.

Cybersecurity Policy Exercise Memo and Presentation
Student teams will draft a joint information security decision memo for their sector based on the cyber policy exercise scenario provided in class. The source material for this memo will be researched throughout the class as a series of weekly assignments. Final memo should be approximately 5-10 pages. The final day of class, student teams will give a 15 minute presentation on their recommendations, and respond to changes in the scenario.

Taping or Recording of Classroom Activities
No student may record or tape any classroom activity without the express written consent of the instructor. If a student believes that he/she is disabled and needs to record or tape classroom activities, he/she should contact the Office of Disability Resources to request an appropriate accommodation.
Daily Schedule

Day 1: Background and history of information security
Why are we here? Why does this matter? What is cybersecurity policy?

Information security is not a new topic – rather it has been around since the invention of the secret, the lie, the deception and the invention. The maxim “knowledge is power” is known well by those who seek to take and keep power. The proliferation of knowledge online has merely amplified this centuries-old truism and brought the realities of global information politics to your desktop.

This day will provide a high level overview of cybersecurity policy and information security management basics, from technical controls to risk management concepts. This day will also provide a brief overview of the most pressing cybersecurity topics and affected sectors. Finally the day will conclude with an introduction into recent events that predicated today’s current information security landscape.

Required Pre-Reading:
- Statement by the President on the Cybersecurity Framework
  http://www.whitehouse.gov/the-press-office/2014/02/12/statement-president-cybersecurity-framework
- Cybersecurity as Realpolitik, Dan Geer
  http://geer.tinho.net/geer.blackhat.6viii14.txt
  - Video: https://www.youtube.com/watch?v=nT-TGvYOBI
- CSIS Significant Cybersecurity Incidents since 2006
  http://csis.org/program/significant-cyber-events

Additional Reading:
- Remarks by the President on Securing Our Nation’s Cyber Infrastructure at
- Cyberspace Policy Review
  - Cyberspace Policy Review – Source Documents
    http://www.whitehouse.gov/cyberreview/documents
- CSIS Significant Cybersecurity Incidents since 2006
  http://csis.org/program/significant-cyber-events

Assignment due Day 2
- Select and write 1-2 pages on an information security topic of interest related to a specific sector, preferably one related to your experience, interest, or relevant to
your current internship. Identify current events, incidents, issues, risks, legislation, policies and regulations influencing the topic.

Day 2: Overview of the national security structure

How is cybersecurity policy created?

The national security apparatus of the United States recognized the importance of information dominance and cybersecurity with the standup of the National Security Agency and the intelligence community in the Cold War. Now the world of secrets has been brought center stage, through recent revelations of national security structures, organizations and capabilities.

This day will focus on current national-level cybersecurity topics and issues and the structure of the National Security Council, the structure of the Executive Office of the President, and the inner-workings of the White House, Intelligence Community, and Executive Agencies. This day will also cover insider threats, information sharing and equities balance, and national plans and strategies.

Required Pre-Reading:
- The National Security Council: An Organizational Assessment
- PPD-1 Organization of the National Security Council System
  https://fas.org/irp/offdocs/ppd/ppd-1.pdf
- National Strategy for Information Sharing and Safeguarding
  http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf
- STIX Introductory Brochure
  http://makingsecuritymeasurable.mitre.org/docs/stix-intro-handout.pdf
- Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis
  http://www.fas.org/sgp/crs/misc/R43821.pdf

Additional Reading:
- PPD-21 Critical Infrastructure Security and Resilience
- Cybersecurity: Authoritative Reports and Resources (October 14, 2014)
  http://www.fas.org/sgp/crs/misc/R42507.pdf
- National Exercise Program 2014
  - Cyber Guard 14-1
- Insider Fraud in Financial Services
  http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=28204
  http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34017

Assignment due Day 3
Day 3: Current state of Cybersecurity

What are the biggest challenges, issues, trends in cybersecurity policy?

This day will discuss the current state of cybersecurity. This will include a discussion of critical infrastructure sectors and other critical sectors affected by cybersecurity policy. Topics will include national-level cybersecurity issues of note, and specific programs and initiatives within sectors. Discussions include specific sector examples to provide students with exposure to the current risks, vulnerabilities, and the threat landscape.

Detailed discussions on information operations and specific threat actors, including organized crime, nation-states, hacktivism, and cyber espionage. We will cover several recent large-scale incidents, and some of the public and private sector information sharing initiatives, roles and responsibilities. Finally, we will discuss privacy, current and proposed legislation, the track record of the Presidential Administration and the history and role of the Cybersecurity Coordinator.

Required Pre-Reading:
- Cyber Matters for Everyone [http://www.brookings.edu/research/podcasts/2014/01/cyber-matters-for-everyone](http://www.brookings.edu/research/podcasts/2014/01/cyber-matters-for-everyone)

Additional Reading:
- Cyberwar and Peace: Hacking Can Reduce Real-World Violence [http://search.proquest.com.proxy.library.cmu.edu/docview/1450255065](http://search.proquest.com.proxy.library.cmu.edu/docview/1450255065)
- Operational Levels of Cyber Intelligence (INSA) [http://www.insaonline.org/i/d/a/b/CyberIntel_embed.aspx](http://www.insaonline.org/i/d/a/b/CyberIntel_embed.aspx)

Assignment due Day 4
- Identify major cybersecurity policy issues affecting your topic and sector. Identify relevant actors and stakeholders. These may be individuals, organizations (sanctioned, criminal, political, etc.), critical infrastructure sectors, and nations.
Identify recent legislative and regulatory changes affecting your sector, and the biggest challenges, issues and trends within your sector. What issues have the most impact? What is at greatest risk? What are the weak points? Draft a brief recommendation to address your identified area of greatest risk that will have the highest likelihood of mitigating your identified risk.

Day 4: Incident Response, Electronic Crimes, and Crisis Communications

You are hacked, now what?

Every organization will experience a cybersecurity issue or incident at some time. The question is not a matter of if but when, and at that time the way the organization responds will dictate their success and survival through the cybersecurity incident.

This day will address critical elements to responding to a cybersecurity incident through crisis communication. Topics will include regulatory engagement, press and client outreach, legislative relations. Case studies include historical and current incidents of note, including privacy breaches, corporate intrusions, online heists and other current high profile cybersecurity incidents. This will also include a discussion on preparation for those incidents, including cyber exercises, gaming, competitions and contingency planning, to prepare you for dealing with the inevitable cybersecurity incident and exercise at the end of this class.

Required Pre-Reading:

- A “Kill Chain” Analysis of the 2013 Target Data Breach [http://docs.ismgcorp.com/files/external/Target_Kill_Chain_Analysis_FINAL.pdf](http://docs.ismgcorp.com/files/external/Target_Kill_Chain_Analysis_FINAL.pdf)

Additional Reading:


Assignment due Day 5
• Identify a current (public) incident associated with your topic, and document the actors, scenario, and circumstances surrounding the incident. Then determine the appropriate mitigating factors, both technical and strategic. Draft a crisis action plan to address your chosen scenario.

Day 5: Enterprise Governance & Strategic Planning
*What is the latest thinking to address the cybersecurity challenge?*
Information security risk management – cyber-risk management – has matured from a technical topic to a business issue at the forefront of leadership concerns. From captains of industry to government policy wonks, the field of information security management is maturing to incorporate theories, models, metrics, and oversight functions to manage cyber-risks through formalized and repeatable practices.

This class will discuss the current state of enterprise governance & strategic planning for cyber risk management, including an overview of risk management frameworks, regulations, and the use of security metrics, both those used by the federal government to measure security effectiveness and best practices from industry. This class will also discuss current models to build an organization’s cyber-risk management strategy, including maturity models, resiliency, and data privacy.

Required Pre-Reading:
• NIST Framework for Improving Critical Infrastructure Cybersecurity
• Cyber Cross Agency Priority Goal
• 2015 DHS FISMA metrics
• Beyond data breaches: global interconnections of cyber risk
• Cyber Risk – A Global Systemic Threat

Additional Reading:
• Is a public health framework the cure for cyber security?
• Cyber Insurance Metrics
• Defense Science Board – Resilient Military Systems and the Advanced Cyber Threat
Assignment due Day 6

- You are the chief of cyber strategy for your organization. Identify the most pressing cyber-risk management issues facing your topic and sector. Identify frameworks and models to help address your issues, and draft a strategy to help manage your organization’s cyber-risk. What frameworks and regulations affect your topic, and what governance practices will you need to implement them?

Day 6: Partnerships

*Headline: We are not in this alone.*

This day will discuss industry engagement to share information amongst peers in the industry, with third parties, and with the Federal government. Information sharing applies for the exchange of threat and vulnerability information, and this discussion will cover several public/private partnerships. Additionally this discussion will cover third party risk management, systemic risk exposure to the sector, and supply chain security.

**Required Pre-Reading:**

- International Strategy for Cyberspace
  http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
- National Infrastructure Protection Plan (NIPP) 2013

**Additional Reading:**

  - March 26, 2013 Steven R. Chabinsky
    www.hsgac.senate.gov/download/?id=c25b7532-6e65-4686-b65e-bc8e2f16869f

- Role of information sharing and analysis centers (ISACs) in private/public sector critical infrastructure protection
  http://www.isaccouncil.org/images/ISAC_Role_in_CIP.pdf

- National Initiative for Cybersecurity Education (NICE) Framework
  http://csrc.nist.gov/nice/framework/
- European Cyber Strategy, UK Cyber Strategy, Australian Cyber Strategy, Canadian Cyber Strategy, DON Cyber Strategy (Pick 2, or similar)

Assignment due Day 7
- Draft a policy paper and recommendation based on the in-class cybersecurity exercise scenario. Incorporate elements from the previous assignments.
- Prepare a 15 minute presentation of your recommendation before the panel of judges.

Day 7: Cybersecurity Policy Exercise (Exam)
This class will include the final cybersecurity policy exercise.