Instructors
Earl Crane
crane@andrew.cmu.edu

Robert Novy
rnovy@andrew.cmu.edu

Time & Location
March 14, 2016 – May 2, 2016 (8 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 critical infrastructure sector of interest
• 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 and how it impacts their critical infrastructure sector of interest
• As a group write a paper and deliver a presentation on the impacts of cybersecurity policy as it relates to their critical infrastructure sector of interest and recommendations for improvement

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.
Dr. Earl Crane is the co-Founder and the Chief Executive Officer of Emergent Network Defense, Inc. (END). Dr. Crane has advised the President of the United States as the Director for Federal Cybersecurity Policy on the White House National Security Council, Wall Street executives and multiple Fortune 100 corporations on their cyber defensive strategies. Dr. Crane led the implementation of the Department of Homeland Security’s information security strategy, and has taught hundreds of cybersecurity masters students and executives through Carnegie Mellon’s Heinz College and CISO Certificate program. He earned his Ph.D. from George Washington University, a Masters of Information System Management at Carnegie Mellon University and a B.S. in mechanical engineering at Carnegie Mellon University. He is helping organizations engage in cybersecurity discussions with impact to their real-world challenges and enable executives to reduce their corporate cybersecurity risk.
Robert Novy
Robert Novy has over 27 years of federal government experience and is currently with the Department of Homeland Security where he focuses on cyber policy, strategy, and operations with regard to investigations and protection.

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 prior 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>14 March</td>
<td>Background and Overview</td>
</tr>
<tr>
<td>Week 2</td>
<td>21 March</td>
<td>National Cybersecurity Policy</td>
</tr>
<tr>
<td>Week 3</td>
<td>28 March</td>
<td>Assets and Vulnerabilities</td>
</tr>
<tr>
<td>Week 4</td>
<td>4 April</td>
<td>Threats and Impacts</td>
</tr>
<tr>
<td>Week</td>
<td>Date</td>
<td>Topic</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
<td>--------------------------------------------------------------</td>
</tr>
<tr>
<td>Week 5</td>
<td>11 April</td>
<td>Managing Risk: Balancing Privacy &amp; Security</td>
</tr>
<tr>
<td>Week 6</td>
<td>18 April</td>
<td>Information Sharing, Partnership, Incident Response and Crisis Management</td>
</tr>
<tr>
<td>Week 7</td>
<td>25 April</td>
<td>Enterprise Governance</td>
</tr>
<tr>
<td>Week 8</td>
<td>2 May</td>
<td>Group Presentations &amp; Paper Submissions (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: 60%
Cyber Policy Paper: 25%
Cyber Policy Presentation: 15%

*Attendance Policy*

Students should attend all classes and comment on other student postings on blackboard. Class participation each day is worth up to 5% each day. 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 Paper and Presentation
Student teams will draft a cybersecurity policy paper for their sector. 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. Good references here and here.

Weekly Assignments
Students will work individually to complete a weekly assignment – a policy brief based on an assigned topic for their sector or topic. Each brief should be 1-2 pages in length, and focus on the specific issue at hand, the challenges of the problem, and a recommended solution.

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:
- At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues: [http://www.nap.edu/read/18749](http://www.nap.edu/read/18749) (Ch 1, 3, 4)
- CSIS Significant Cybersecurity Incidents since 2006 [http://csis.org/program/significant-cyber-events](http://csis.org/program/significant-cyber-events)

Additional Reference Material:
- Cybersecurity as Realpolitik, Dan Geer [http://geer.tinho.net/geer.blackhat.6viii14.txt](http://geer.tinho.net/geer.blackhat.6viii14.txt)
  - Video: [https://www.youtube.com/watch?v=nT-TGvYOBpI](https://www.youtube.com/watch?v=nT-TGvYOBpI)

Assignment #1 (Due at the beginning of class on day 2 – please submit via blackboard.)
- Form teams and select a critical infrastructure sector of interest.
- Select and individually write a policy brief on an information security topic of interest related to your specific sector, preferably one related to your experience, interest, or relevant to your current internship. What is the current state of cybersecurity in your sector? Identify current events, incidents, issues, risks, legislation, policies and regulations influencing the topic.
Day 2: Overview of current and past national cybersecurity policy and the national security “policy-making structure”

How is cybersecurity policy created? Discuss current and past policy.

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 and past national-level cybersecurity policy topics and issues as well as 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 the White House Cybersecurity National Action Plan which was implemented to “take near-term actions and puts in place a long term strategy to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security.”

Required Pre-Reading:
- PPD-1 Organization of the National Security Council System [https://fas.org/irp/offdocs/ppd/ppd-1.pdf](https://fas.org/irp/offdocs/ppd/ppd-1.pdf)

Additional Reference Material:
- Cybersecurity: Authoritative Reports and Resources (October 14, 2014) [http://www.fas.org/sgp/crs/misc/R42507.pdf](http://www.fas.org/sgp/crs/misc/R42507.pdf)
Assignment #2 (Due at the beginning of class on day 3 – please submit via blackboard.)

- Write a policy brief to a key decision maker related to your critical infrastructure sector of interest. This key decision maker could be a leader of your agency, the CEO of your company, or the Director of your nonprofit organization. Identify equities, parties, policies, regulations, standards, and guidelines from the White House’s Cybersecurity National Action Plan (Factsheet) and related links that are relevant or impact your critical infrastructure sector of interest. From your review of the Cybersecurity National Action Plan, provide a single policy recommendation based on your assessment and analysis of the plan that impacts your sector.
**Day 3: Assets & Vulnerabilities**  
*What are we trying to protect, and why is this so hard?*

Crown Jewels, Intellectual Property, and Personally Identifiable Information – the gold of the digital age is stored in 1’s and 0’s. This day will discuss the current state of cybersecurity in general, national-level cybersecurity issues of note, and specific programs and initiatives within sectors.

**Required Pre-Reading:**

**Additional Reference Material:**
- 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)

**Assignment #3 (Due at the beginning of class on day 4 – please submit via blackboard.**
- Identify the “crown jewels” of your sector or topic and prepare a policy brief discussing the state of their security. How important are these assets and to which stakeholders? These may be individuals, organizations (sanctioned, criminal, political, etc.), critical infrastructure sectors, and nations. What are the greatest vulnerabilities and challenges in addressing those vulnerabilities? Draft a brief recommendation of how to protect your most valuable assets.
Day 4:
Threats & Impacts

Who and what are the threats?

Whether it is a nation state attack, extortion, data destruction, payment card data breaches or the theft of personally identifiable information (PII), the threat of these crimes or attacks will continue.

This day will address current cyber threats and the impacts. The discussion will focus on today’s threat actors and their tactics, techniques, protocols and target sets. Discussions will include the evolution of the threat, cybercrime, hacktivism, and cyber espionage.

Required Pre-Reading:

Additional Reference Material:
- A “Kill Chain” Analysis of the 2013 Target Data Breach http://docs.ismgcorp.com/files/external/Target_Kill_Chain_Analysis_FINAL.pdf

Assignment #4 (Due at the beginning of class on day 5 – please submit via blackboard.)
- Write a policy brief to a key decision maker which discusses the known cyber threats impacting your critical infrastructure sector of interest. Describe the publicly known threats targeting your sector including actors, tactics, techniques, and protocols. Also describe what you believe to be their intended target or what they hope to achieve. Provide one policy recommendation which could help your sector reduce or counter one of the threats impacting your critical infrastructure sector of interest.
Day 5:  
Managing Risk: Balancing Privacy and Security  
*How do we get clarity through the gray?*

This day will discuss risk management. In cybersecurity, there is always a balance that must be struck between security, privacy, and operations. This balance is now the center of a national debate and requires policy expertise, insight, and recommendations. Risk discussions will include how cybersecurity risk is managed, mitigated, transferred or accepted, and the challenges between balancing privacy and security.

Required Pre-Reading:
- NIST SP 800-39: Managing Information Security Risk:  
- Governing Cyberspace: A Road Map for Transatlantic Leadership:  
  [http://carnegieendowment.org/2016/01/18/governing-cyberspace-road-map-for-transatlantic-leadership/issj](http://carnegieendowment.org/2016/01/18/governing-cyberspace-road-map-for-transatlantic-leadership/issj) (Ch 1)
- Congressional Hearing – March 1, 2016, House Judiciary Committee  
  The Encryption Tightrope: Balancing Americans’ Security and Privacy  
  Written Testimony:  
  FBI Director James Comey  
  [http://judiciary.house.gov/_cache/files/781b192e-78b3-41b8-ad6c-0e01e578c0eb/comey-written-testimony.pdf](http://judiciary.house.gov/_cache/files/781b192e-78b3-41b8-ad6c-0e01e578c0eb/comey-written-testimony.pdf)  
  Mr. Bruce Sewell, Apple Inc.  
  Cyrus R. Vance Jr., District Attorney, New York County, NY  
  Susan Landau, PhD, Worcester Polytechnic Institute  

Additional Reference Material:
- Principles for Effective Cybersecurity Regulatory Guidance  
- Data Privacy—Protecting This Asset Is a Priority:  
- The Ground Truth About Encryption, The Chertoff Group  
- Smartphone Encryption and Public Safety – Manhattan DA Report  
Assignment #5 (Due at the beginning of class on day 6 – please submit via blackboard.)

- Write a policy brief which discusses risk management related to your critical infrastructure sector of interest. What are the privacy concerns organizations and businesses in your sector must take into consideration? How does your sector of interest balance privacy and security?
Day 6:
Information Sharing, Partnership, Incident Response and Crisis Management

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, 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. We will address critical elements to responding to a cybersecurity incident through crisis management and communication. Topics will include regulatory engagement, press and client outreach. 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 for dealing with the inevitable cybersecurity incident.

Required Pre-Reading:

- Mitigate cyber-attacks with crisis management
- Department of Justice – Best Practices for Victim Response and Reporting Cyber Incidents
- DHS Cyber Incident Response

Additional Reference Material:

- MS-ISAC Incident Response Guide
- March 26, 2013 Steven R. Chabinsky
  [Link: www.hsgac.senate.gov/download/?id=c25b7532-6e65-4686-b65e-bc8e2f16869f]

- FBI Cyber Division
  [Link: https://www.fbi.gov/about-us/investigate/cyber/cyber]

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

- International Strategy for Cyberspace
  [Link: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf]

Assignment #6 (Due at the beginning of class on day 7 – please submit via blackboard.)

- Identify a current (public) incident associated with your critical infrastructure sector of interest, and document the actors, scenario, and circumstances surrounding the incident. Hint - information and research from Assignment #4 may be helpful. Determine the appropriate mitigating factors, both technical and strategic. Draft an incident response and crisis action plan to address your chosen scenario. Document the partnerships and information sharing that would be helpful before, during, and after an incident that is relevant to your critical infrastructure sector of interest.
Day 7:
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:
- Understanding and Communicating Risk Appetite – COSO:
- RIMS: Exploring Risk Appetite and Risk Tolerance:
- NACD: Cyber Risk Oversight:

Additional Reference Material:
- Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool Overview:
  o Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool:
- 2016 DHS FISMA metrics:
  https://www.dhs.gov/sites/default/files/publications/FY%202016%20CIO%20FISMA%20Metrics%20v1.0.pdf
- Cyber Cross Agency Priority Goal:
  https://www.performance.gov/node/3401/view?view=public#overview
• Cyber Insurance Metrics:
• Defense Science Board – Resilient Military Systems and the Advanced Cyber Threat
• Cyber Risk – A Global Systemic Threat

Assignment #7 (Due at the beginning of class on day 6 – please submit via blackboard.)
  • Final project: Cybersecurity Policy Paper and Presentation
Day 8: Cybersecurity Policy Group Presentations (Exam)
This class will include the final cybersecurity policy group presentations.