Fall 2023

CS 648: Cyber Security Investigations & Law

Sean Walsh

The Interface and Implications of Internet /Cyber Network Relationships on Security and Investigations

The focus of this course is to prepare students for the real life experiences of those responsible for operating and protecting communication and data storage systems. The course will provide the student with a methodology to examine and investigate intrusions of data storage, data management, and data transmission systems as a part of an integrated network. We will explore the various interfaces of these systems from a technical, human, investigative, and potential legal concerns. The course will provide the student with various fundamental legal knowledge necessary for a cyber practitioner: (a) basic intellectual property law including trade secrets and patents; (b) foreign viewpoints of intellectual property and compliance to include EU privacy law; (c) U.S. law of electronic surveillance, electronic search, and stored communications; (d) government and workplace consensual search and surveillance and consent banners/agreements.

The course requires the students to actively participate in class to explore system vulnerabilities and design solutions including the use of encryption. While preparing these solutions, students will be expected that their solutions will comport with legal requirements.

The course is designed to enhance the students skill at recognizing cyber security issues, investigating intrusions, and legal concerns that may arise in the course of an investigation or designing a network.

I will not be using a textbook per se. Instead for all the "legal" materials, I will provide links or copies on line to be downloaded. As for articles technical and discussion on each of the various subjects the information they will be downloadable. My PPT will be made available to the students.

NOTHING IN THIS COURSE WRITTEN OR ORAL SHALL BE CONSIDERED AS LEGAL ADVISE or should it be taken as such.

Requirements: Students are expected to have a basic foundation in computer and cyber networks as a course prerequisite. Students are expected to be active class participants; this will constitute one third of their grade. A written examine in October will constitute another one third of their grade. There will be a final written examine which will encompass the entire course material.

- **Week One** Introduction to recognizing proprietary information and the means to protect such information: Trade Secrets, Copy Right, and Trade Mark. Government classification system and handling classified documents. Nondisclosure and employment agreements and post employment nondisclosure or restrictions. (3 Hrs.)
- **Week Two** Study the theory and types of Emanations and the Electromagnetic Spectrum. Examine which parts of the spectrum are governed by privacy laws.
- **Week Three** Review of mandated data protection requirements for various industries, e.g., medical, financial, government records, and private nondisclosure agreements. In addition to the technical and legal element, we will examine the human part of this equation in accomplishing these requirements. (3 Hrs.)
- **Week Four** Have the students map out the various types of computing devices and how they interconnect from both a personal user and from a corporate environment. (3 Hrs.)

- **Week Five** Have the students map out the various types of network telecommunications that may link these systems to other systems mapped in week four. (3 Hrs.)
- **Week Six** We will study the history and the role of cryptology. We will then discuss the use of modern crypto technology as a solution to secure OS vulnerabilities and enhance privacy vs. the risks to society. (3 Hrs.)
- **Week Seven** The students will combine the models developed in weeks Four and Five overlaying them models to see how they interrelate and find vulnerabilities. (3 Hrs.)
- **Week Eight** We will do an overview of the US Criminal laws and the EU Privacy laws governing these systems in order that you will understand what you may and may not do to protect IP or your system. Intellectual Property, PPI, and the jurisdiction aspects of stored data will be covered in this segment. (3 Hrs.)
- **Weeks Nine & Ten** We will return to our model and insert the controlling legal authorities for each part of the system in order to examine the correlation of our known vulnerabilities with the duty to protect within the constrains of the law. The class will apply cryptology as a solution and explore its vulnerabilities. The students will then discuss how as a systems administrator / CIO need to address these issues and anticipate them. (6 Hrs.)
- **Week Eleven** Examine the "Insider Threat." Study the hidden threat to cyber security the "Supply Chain." What is a supply chain and whose responsibility is it to account for its threat. We will discuss the practicality of enforcing security / nondisclosure / contractual agreements down a supply chain. (3 Hrs.)
- **Week Twelve** We will examine Import and Export restrictions as it relates to hardware and software technology. Will this after our model solutions. In addition, we will include how to respond to service of legal process and export import restrictions. (3 Hrs.)
- **Week Thirteen** Now with a better understanding of interrelationships of the risk model how do we defend against attacks and conduct intrusion investigations. We will explore various private security and law enforcement methods to combat intrusions. Based on what you learned to date, you will also learn to construct a consent agreement for a third party to have access to or remove data from your system and the limits on you to do so. (3 Hrs.)
- **Week Fourteen** Cyber attacks, the role of the nation-state. When does intrusions rise to an act of war? What counterattacks are justified? How do we measure collateral damage of our counterattacks? Can private individuals or corporations counter attack or only nation-states? We conclude with a quick review of the course and answer any open questions (3 Hrs.)