# Security

Security: Managing, Protecting, and Assuring Sensitive Information Assets

Instructors:

**Craig Blaha**

Phone: (512) 633-9745 – this is my cell, please use judiciously and don’t share outside of our class!

Email: [craig.blaha@utexas.edu](mailto:craig.blaha@utexas.edu)

Office Hours: By Appointment

TA: TBD

Office Hours: TBD

## Course Location and Meeting Times: ECJ 1.312 on Fridays and EER 1.518 on Saturdays

8:00 AM – 12:00 PM

* Weekend 1: August 27 - 28 (virtual)
* Weekend 2: September 17 - 18
* Weekend 3: October 15 - 16
* Weekend 4: November 12 - 13
* Weekend 5: December 3 – 4



## **I**. Recommended (NOT required) Reading List

1. *Cryptography and Network Security*, 6th ed., Stallings, W. Pearson, 2013.
2. *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats*, Donaldson, S., Siegel, S., et. al. Apress, 2015.

Due to the dynamic nature of information security, this course will utilize extensive supplemental readings in current cybersecurity and identity topics, including journal articles, news reports, blogs, and industry publications. These readings will be selected and assigned closer to the actual course dates and throughout the semester.

## II. Course Aims and Objectives:

### Aims:

This course aims to prepare students for leadership roles in identity related, network and information technology firms. Students will understand common information security architecture, tools, concepts, and terminology

This course provides students in the MSIMS program a foundational understanding of the theory, concepts, and practical applications of information security and its relationship to identity management. Focused on the people, processes, and technologies that support today’s organizational cybersecurity programs, this course prepares students for leadership roles in the protection of sensitive information assets. Students will leave this course with a solid understanding of the history of information security; the threats and challenges that cybersecurity programs face today; methods, tools, and architectures used to create successful cybersecurity programs in industry, government, and not-for-profit organizations; and the skills and techniques for governing a strategic enterprise information security program. Students completing the course will be well prepared for careers in identity management, network security operations, enterprise security program management, and enterprise information technology risk management. This course combines theoretical with practical readings and exercises, and includes explanations of both technical and non-technical security concepts and practices.

### Specific Learning Objectives:

By the end of this course, students will:

1. Understand how information is communicated via the Internet, the operation of its essential components, the operation of its security services, and how those services are implemented.
2. Be able to manage an organization wide risk assessment, including managing security related network scans.
3. Understand the general historical development of information security as a discipline, with specific focus on the evolution of information security in the context of computing, networking, and the Internet.
4. Understand how information is stored and processed in computer systems, and the security implications of these activities
5. Understand how information is transmitted and managed over networks, including the Internet, and how the essential components of these networks operate
6. Understand the theoretical components of information security, particularly *confidentiality*, *integrity*, and *availability*, and how these components are incorporated into security technologies and management programs
7. Understand the structure and functions of an enterprise cybersecurity program, including:
   1. Security Program Management
   2. Security Risks and Threats
   3. Security Controls and Technologies
   4. Security Program Monitoring and Evaluation
8. Apply the concepts and techniques of information security to a variety of cases, scenarios, and exercises, demonstrating knowledge through class discussion, papers and presentations, and the completion of technical security lab exercises.

## III. Course Topics

Information security is a dynamic field, which changes frequently as new threats and countermeasures are incorporated into our information environment. That being said, one may identify general category topics that continuously remain relevant for information security professionals, even as their details change with time. These include:

* 1. Security governance, leadership, and strategy – management, at an executive level, of an organization’s information security program
  2. Security policies and standards – bureaucratic and organizational architectures designed to standardize information security program practices
  3. Compliance and audit – external and internal review of organizational activities against defined frameworks and regimes for standardized behavior
  4. Security risk and threat management – the identification and analysis of how security problems or failures may impact the organization
  5. People-centric security – the process of training and managing people to ensure proper security behaviors and culture, and maximizing the value of human capital in support of protecting information assets
  6. Security in endpoints and devices – how security functions at the level of information technology, including servers, personal computers, network devices, and mobile devices
  7. Network security – how security functions as information flows between devices in a networked infrastructure such as the Internet
  8. Cryptography – the practice of protecting and verifying information using encryption systems and algorithms
  9. Information asset management and classification – the practice of understanding and managing the value of an organization’s information, and protecting sensitive assets from loss or damage
  10. Identity and access management – the means by which people and systems are allowed to use or control specific information assets
  11. Physical security – the protection of physical and environmental infrastructures from threats and risks
  12. Malware – the challenges of malicious code, including viruses, worms, spyware, and other software-based threats
  13. Security monitoring and logging – visibility into an organization’s digital environment for the purposes of managing information use and detecting attacks and other failures
  14. Security vulnerability management – the practice of identifying and managing weaknesses in an infrastructure that may be exploited by an attacker
  15. Security incident response – the practice of managing and recovering from a security failure, including data loss, damage, or theft
  16. Business continuity and disaster recovery – the ability of an organization to maintain and continue operations in the wake of a disaster or other incident that degrades or destroys organizational capabilities
  17. Legal implications of information security – the practice of understanding and managing information security at a policy and regulatory level, as well as the legal implications of security decisions and activities

## IV. Course Schedule:

|  |  |
| --- | --- |
| Meeting # | Main Topic(s) |
| **1 – August 27** | **Introduction**  Course Introduction and Structure  Discussion of Enterprise Security part 1  In class exercise – newly hired CISO |
| **2 – August 28** | **Information Security Overview**  Discussion of Enterprise Security part 2  Start OTW  Homework – read one book, follow one blog, progress on OTW  For 9/17, prepare case study #1  Prepare Ransomware elevator pitch |
| **3 – September 17** | **Networking Part 1**  IP addressing, public and private IP address concepts  Ports and protocols  Threat detection and prevention  Threat vectors  In class exercises/tasks  Ransomware pitch and discussion |
| **4 – September 18** | **Networking Part 2**  CIA, PPT, GRC  Student Case Study Presentations  Case study in class exercise  Homework – blog, book, OTW  CIA Due 10/15  Prepare Cloud elevator pitch |
| **5 – October 15** | **Applied Encryption**  Diffie Hellman/El Gamal,  Back doors, internet of things, spoofing  Cloud pitch and discussion |
| **6 – Oct 16** | **Applied Encryption 2**  RSA, and Elliptical Curve Cryptography  Physical Security  Case study discussion and presentation  Homework – blog, book, OTW  Prepare Two Factor elevator pitch  PPT Due 11/12 |
| **7 – Nov 12** | **ID, Authn, Authz, and Access Management 1**  Two factor pitch and discussion |
| **8 – Nov 13** | **ID, Authn, Authz, and Access Management 2**  Case study discussion and presentation  Homework – blog, book, OTW  GRC Due 12/3 |
| **9 – Dec 3** | **Course Wrap-up**  Redundancy and Disaster Recovery  Social Engineering, User Education, Facilities Security  Policies and Procedures  Case study presentations |
| **10 – Dec 4** | **Course Wrap-up**  Elevator pitch roulette |

## V. Grading Procedures: Grades will be based on:

1. (20%) Participation
2. (20%) Weekly reading
3. (20%) 4 case studies (write-ups & presentations)
4. (20%) Key topics oral presentations/elevator pitches
5. (10%) 1 OTW lab journal kept throughout the class (Canvas)
6. (10%) Breach Detection Exercise

## VI. Assignments

1. Participation
   1. Your active and positive participation in the class will count as 20% of your grade.
2. Weekly Reading
   1. As an information security professional, you will need to develop a habit of reading as much as possible in order to be aware of the latest threats and vulnerabilities. Your homework for this class, therefor, includes reading one book of your choice and following one blog of your choice between sessions, and offering a brief discussion about each on Canvas and in class.
3. Four Case Studies
   1. Your write up and presentation of the four case studies over the course of the semester, using the various lenses we discuss in class, is worth 20% of your grade
4. Key Topics oral presentations/elevator pitch
   1. There are a few key topics we know every security professional should be ready to discuss; ransomware, cloud security, and two factor authentication. Students will work to develop their “elevator pitch” related to each of these topics. Imagine you step into an elevator with the chairperson of the board. They ask you about one of these topics, you have less than three minutes to convince them first that you know what you are talking about, and second that they need to put resources on your plate to address the problem. During the last class weekend you will select, at random (by drawing straws), a pitch that you will give in front of the class. All four of these pitches together count for 20%.
5. Student Lab Journal
   1. Your write up of the in-class labs and exercises will count as 10% of your grade.
6. Breach Detection Exercise
   1. This is a series of quizzes related to networking that will help you apply what we discuss in the class and counts as 10% of your grade.

## VII. Course Policies

Class attendance and participation policy: Students are expected to attend all class sessions and complete all assignments on-time. Exceptions will be made on a case-by-case basis. If attending remotely, students will be expected to be visually present and engaged with the class.

## VIII. Academic Integrity

**University of Texas Honor Code**

The core values of The University of Texas at Austin are learning, discovery, freedom, leadership, individual opportunity, and responsibility. Each member of the university is expected to uphold these values through integrity, honesty, trust, fairness, and respect toward peers and community.

## IX. Other University Notices and Policies

**Use of E-mail for Official Correspondence to Students**

* All students should become familiar with the University's official e-mail student notification policy. It is the student's responsibility to keep the University informed as to changes in his or her e-mail address. Students are expected to check e-mail on a frequent and regular basis in order to stay current with University-related communications, recognizing that certain communications may be time-critical. It is recommended that e-mail be checked daily, but at a minimum, twice per week. The complete text of this policy and instructions for updating your e-mail address are available at [**http://www.utexas.edu/its/help/utmail/1564**](http://www.utexas.edu/its/help/utmail/1564) **.**

**Documented Disability Statement**

Any student with a documented disability who requires academic accommodations should contact Services for Students with Disabilities (SSD) at (512) 471-6259 (voice) or 1-866-329-3986 (video phone). Faculty are not required to provide accommodations without an official accommodation letter from SSD. *(Note to Faculty: Details of a student’s disability are confidential. Faculty should not ask questions related to a student’s condition or diagnosis when receiving an official accommodation letter.)*

* Please notify me as quickly as possible if the material being presented in class is not accessible (e.g., instructional videos need captioning, course packets are not readable for proper alternative text conversion, etc.).
* Please notify me as early in the semester as possible if disability-related accommodations for field trips are required. Advanced notice will permit the arrangement of accommodations on the given day (e.g., transportation, site accessibility, etc.).
* Contact Services for Students with Disabilities at 471-6259 (voice) or 1-866-329-3986 (video phone) or reference SSD’s website for more disability-related information: <http://www.utexas.edu/diversity/ddce/ssd/for_cstudents.php>

**Behavior Concerns Advice Line (BCAL)**

If you are worried about someone who is acting differently, you may use the Behavior Concerns Advice Line to discuss by phone your concerns about another individual’s behavior. This service is provided through a partnership among the Office of the Dean of Students, the Counseling and Mental Health Center (CMHC), the Employee Assistance Program (EAP), and The University of Texas Police Department (UTPD). Call 512-232-5050 or visit <http://www.utexas.edu/safety/bcal>.

**Emergency Evacuation Policy**

Occupants of buildings on the UT Austin campus are required to evacuate and assemble outside when a fire alarm is activated or an announcement is made. Please be aware of the following policies regarding evacuation:

* Familiarize yourself with all exit doors of the classroom and the building. Remember that the nearest exit door may not be the one you used when you entered the building.
* If you require assistance to evacuate, inform me in writing during the first week of class.
* In the event of an evacuation, follow my instructions or those of class instructors.

Do not re-enter a building unless you’re given instructions by the Austin Fire Department, the UT Austin Police Department, or the Fire Prevention Services office.