# ***Information Security***

Managing, Protecting, and Assuring Sensitive Information Assets

Instructor:

**Craig Blaha**

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

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

Office Hours: By Appointment

TA: TBD

Office Hours: By arrangement – send me a note and we will find a time that works!

## Course Location and Meeting Times:

Thompson Conference Center (TCC) Room 3.102

1:00 PM – 5:00 PM

* Weekend 1: August 25 - 26
* Weekend 2: September 22 - 23
* Weekend 3: October 13 - 14
* Weekend 4: November 10 - 11
* Weekend 5: December 1 - 2



## **I**. Reading List

Due to the dynamic nature of information security, this course will utilize extensive supplemental readings in current cybersecurity 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; these resources will all be available at no additional cost (through UT library or the open web).

## II. Course Overview:

This course provides students in the MSISP program a foundational understanding of the theory, concepts, and practical applications of information security. Focused on the people, processes, and technologies that support cybersecurity programs in today’s organizations, 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. This course combines theoretical with practical readings and exercises, and includes explanations of both technical and non-technical security concepts and practices.

Students in this program tend to have a broad range of skills and experience. In my experience, the best learning that happens in class includes active participation from all parties. If you have an experience or expertise that is related to a topic we are covering in class, please share! The most valuable assets in this class are the students, your experience, and your questions. Your fellow students have a lot to learn from you, whether it is from your experience and expertise or from your questions if a topic is new or confusing to you!

### Course Learning Goals:

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

## 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

Assignment of course letter grades is provided below; no rounding will be applied. Although there aren't any extra credit assignments, other options for flexibility are described next.

|  |  |
| --- | --- |
| 90-100 | A |
| 80 - 89 | B |
| 70 - 79 | C |
| 60 - 69 | D |
| 0 – 59 | F |

1. Flexibility
   1. This class is designed around a few assumptions; you are busy professionals with a range of experience in information security. In previous semesters I have had students who claimed to know nothing about the technical components of information security sitting alongside students who have been in charge of information security teams for 10+ years. My goal is to cover the broad range of topics that make up the field of information security and create a flexible course structure that supports the growth of all students in the class. In exchange I ask for three things; communication, participation, and self-directed effort.
      1. My first ask is that you communicate with me as soon as you encounter a problem (work or family schedule, sickness, deployment in the field, etc.). I will work with you to make sure you get as much out of this class as possible given your other constraints, but I need to be aware of the constraints.
      2. The second ask is that you help the other students in the class through your participation; if you have a ton of technical experience, sharing those first-hand stories helps your colleagues learn more quickly than they possibly could from a lecture alone. If you have no technical experience, you still have a lot of other experience, ideas, thoughts, and questions that will help your colleagues see things from a new perspective. Nothing is more valuable than a good question!
      3. Lastly, I ask that you push yourself in the direction you find most valuable. I will work with you on determining this direction, and it doesn’t have to be the same direction as the student sitting next to you. For example, I have had students who had a big, new, technical certification test they had to tackle at the end of the semester. A big component of their effort for this class was preparing for that cert. Others have always wanted to become an expert in a particular technology solution, so they spent time between classes developing that expertise. Use this class to make progress toward your professional goals.

## 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 your reading on Canvas and in class. I use the “book and blog” construct to give you a sense of the minimum amount of reading successful information security leaders have told me they typically undertake each month. We will talk more about whether this reading has to be an actual “book or blog”.
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 multi-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.

## IV. Course Schedule:

|  |  |
| --- | --- |
| Meeting # | Main Topic(s) |
| **1 – August 25** | **Introduction**  Course Introduction and Structure  Discussion of Enterprise Security part 1  In class exercise – newly hired CISO |
| **2 – August 26** | **Information Security Overview**  Discussion of Enterprise Security part 2  Start OTW  Homework – read one book, follow one blog, progress on OTW  For 9/22, prepare case study #1  Prepare Ransomware elevator pitch |
| **3 – September 22** | **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 23** | **Networking Part 2**  CIA, PPT, GRC  Student Case Study Presentations  Case study in class exercise  Homework – blog, book, OTW  CIA Due 10/13  Prepare Cloud elevator pitch |
| **5 – October 13** | **Applied Encryption**  Diffie Hellman/El Gamal,  Back doors, internet of things, spoofing, blockchain  Cloud pitch and discussion |
| **6 – October 14** | **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 11/10 |
| **7 – November 10** | **ID, Authn, Authz, and Access Management 1**  Two factor pitch and discussion |
| **8 – November 11** | **ID, Authn, Authz, and Access Management 2**  Case study discussion and presentation  Homework – blog, book, OTW  GRC Due 12/1 |
| **9 – December 1** | **Course Wrap-up**  Redundancy and Disaster Recovery  Social Engineering, User Education, Facilities Security  Policies and Procedures  Case study presentations |
| **10 – December 2** | **Course Wrap-up**  Elevator pitch roulette |

# University of Texas and MSISP grading policies

## Examinations and Grades

The faculty instructors for each course will determine if exams are necessary as well as exam schedules and grading criteria if exams are included (described above).

## Grading

This course must be taken on a letter grade basis. Candidates for the master’s degree must have a cumulative GPA of at least 3.00 in core courses. Per University policy, any graduate student whose cumulative grade point average falls below 3.00 at the end of any semester will be placed on scholastic warning status, and must bring their cumulative GPA to at least 3.00 during the next semester, or be subject to dismissal from the program.

Official grade point averages are calculated by the UT Registrar and appear on the student’s academic record maintained by the Registrar.

# Learning and Growth

Throughout the course, your learning and growth in theory and practice of the information security and privacy profession are important. We all need accommodations because we all learn differently, and the current pandemic makes accommodations all the more important. If there are aspects of this course that prevent you from learning or exclude you, please let me know as soon as possible. Together we will develop strategies to meet your needs and the course requirements. I also encourage you to reach out to the resources available through UT and the MSISP program. Many are included on this syllabus.

# Academic Integrity

Each student is expected to abide by the UT Honor Code: ``As a student of The University of Texas at Austin, I shall abide by the core values of the University and uphold academic integrity.'' If you use words or ideas that are not your own (or that you have used in a previous class), you must cite your sources. Otherwise, you might be in violation of the university's academic integrity policies. Please see [Student Conduct and Academic Integrity](https://deanofstudents.utexas.edu/conduct/), and talk to me if you are even slightly uncertain!

# Use of Electronics

To help you connect the pieces of the class together, please focus the use of electronics on course related activities.

# Video Recordings

Video recording of class activities are reserved for students and TAs in this class only for educational purposes and are protected by [FERPA](https://registrar.utexas.edu/staff/ferpa) laws if any students are identifiable in the video. Video recordings should not be shared outside the class in any form. Students violating this university policy could face misconduct proceedings.

# Students with Disabilities

The university is committed to creating an accessible and inclusive learning environment consistent with university policy and federal and state law. Please let me know if you experience any barriers to learning so I can work with you to ensure you have equal opportunity to participate fully in this course. If you are a student with a disability, or think you may have a disability, and need accommodations please contact [Services for Students with Disabilities](https://diversity.utexas.edu/disability/) (SSD). Here are some [examples](https://diversity.utexas.edu/disability/about-disabilities/) of the types of diagnoses and conditions that can be considered disabilities:[Attention-Deficit/Hyperactivity Disorders (ADHD)](https://diversity.utexas.edu/disability/adhd), [Autism](https://diversity.utexas.edu/disability/students-with-austism-spectrum-disorders/), [Blind & Visually Impaired](https://diversity.utexas.edu/disability/visual-impairments/), [Brain Injuries](https://diversity.utexas.edu/disability/traumatic-brain-injuries/), [Deaf & Hard of Hearing](https://diversity.utexas.edu/disability/deaf-and-hard-of-hearing/), [Learning Disabilities](https://diversity.utexas.edu/disability/learning-disabilities/), [Medical Disabilities](https://diversity.utexas.edu/disability/medical-disabilities/), [Physical Disabilities](https://diversity.utexas.edu/disability/physical-disabilities/),[Psychological Disabilities](https://diversity.utexas.edu/disability/psychological-disabilities-2/) and [Temporary Disabilities](https://diversity.utexas.edu/disability/temporary-disabilities/). Please refer to SSD's [website](https://diversity.utexas.edu/disability/) for contact and more information. If you are already registered with SSD, please deliver your Accommodation Letter to me as early as possible in the semester so we can discuss your approved accommodations and needs in this course.

# Mental Health Counseling

Graduate school can be stressful and sometimes we need a little help. Luckily, we have a wealth of resources and dedicated people ready to assist you, and treatment does work. The [Counseling and Mental Health Center](https://cmhc.utexas.edu/index.html) provides counseling, psychiatric, consultation, and prevention services that facilitate academic and life goals and enhance personal growth and well-being. Counselors are available Monday-Friday 8am-5pm by phone (512-471-3515) and Zoom.

If you are experiencing a mental health crisis (e.g. depression or anxiety), please call the Mental Health Center Crisis line at 512-471-CALL(2255). Call even if you aren't sure you're in a full-blown crisis, but sincerely need help. Staff are there to help you.

# Student Rights and Responsibilities

* You have a right to a learning environment that supports mental and physical wellness.
* You have a right to respect.
* You have a right to be assessed and graded fairly.
* You have a right to freedom of opinion and expression.
* You have a right to privacy and confidentiality.
* You have a right to meaningful and equal participation, to self-organize groups to improve your learning environment.
* You have a right to learn in an environment that is welcoming to all people. No student shall be isolated, excluded or diminished in any way.

With these rights come responsibilities:

* You are responsible for taking care of yourself, managing your time, and communicating with the teaching team and others if things start to feel out of control or overwhelming.
* You are responsible for acting in a way that is worthy of respect and always respectful of others.
* Your experience with this course is directly related to the quality of the energy that you bring to it, and your energy shapes the quality of your peers' experiences.
* You are responsible for creating an inclusive environment and for speaking up when someone is excluded.
* You are responsible for holding yourself accountable to these standards, holding each other to these standards, and holding the teaching team accountable as well.

# Official Correspondence

UT Austin [considers e-mail as an official mode of university correspondence](https://cio.utexas.edu/policies/university-electronic-mail-student-notification-policy). You are responsible for following course-related information on the course Canvas site.

# Religious Holy Days

In accordance with [section 51.911 of the Texas Education code](https://texas.public.law/statutes/tex._educ._code_section_51.911) and [University policies on class attendance](https://catalog.utexas.edu/general-information/academic-policies-and-procedures/attendance/), a student who misses classes or other required activities, including examinations, for the observance of a religious holy day should inform the instructor as far in advance of the absence as possible so that arrangements can be made to complete an assignment within a reasonable period after the absence. A reasonable accommodation does not include substantial modification to academic standards, or adjustments of requirements essential to any program of instruction. Students and instructors who have questions or concerns about academic accommodations for religious observance or religious beliefs may contact the [Office for Inclusion and Equity](https://equity.utexas.edu/). The University does not maintain a list of religious holy days.

# Absence for Military Service

In accordance with [section 51.9111 of the Texas Education code](https://texas.public.law/statutes/tex._educ._code_section_51.9111) and [University policies on class attendance](https://catalog.utexas.edu/general-information/academic-policies-and-procedures/attendance/), a student is excused from attending classes or engaging in other required activities, including exams, if he or she is called to active military service of a reasonably brief duration. The maximum time for which the student may be excused has been defined by the Texas Higher Education Coordinating Board as ``no more than 25 percent of the total number of class meetings or the contact hour equivalent (not including the final examination period) for the specific course or courses in which the student is currently enrolled at the beginning of the period of active military service.'' The student will be allowed a reasonable time after the absence to complete assignments and take exams. Please notify the MSISP program administrators or your faculty members as soon as you are aware of a situation that might impact your ability to actively participate in class. This includes not only deployment and field operations, but internet connection adequate to handle two-way video and voice communications.

# COVID-19 Guidance

To help preserve our in-person learning environment, the university recommends the following.

* Adhere to university [mask guidance](https://utexas.app.box.com/s/ymob0b4vimv4j9gnhskpsqywwadk3f10).

* [Vaccinations are widely available](https://uthealthaustin.org/patient-resources/covid-19-updates/covid-19-vaccination), free and not billed to health insurance. The vaccine will help protect against the transmission of the virus to others and reduce serious symptoms in those who are vaccinated.

* [Proactive Community Testing](https://healthyhorns.utexas.edu/coronavirus_proactive_testing.html) remains an important part of the universityâ€™s efforts to protect our community. Tests are fast and free.
* Visit [Protect Texas Together](http://protect.utexas.edu) for more information

# Safety Information (http://www.utexas.edu/safety)

If you have concerns about the safety or behavior of students, TAs, Professors, or others, call the Behavorial Concerns Advice Line at 512-232-5050. Your call can be anonymous. If something doesn't feel right, it probably isn't. Trust your instincts and share your concerns.

Occupants of buildings are required to evacuate buildings when a fire alarm is activated. Alarm activation or announcement requires exiting and assembling outside.

* Familiarize yourself with all exit doors of each classroom and building you may occupy. The nearest exit door may not be the one you used when entering the building.
* Students requiring assistance in evacuation shall inform their instructor in writing during the first week of class.
* In the event of an evacuation, follow the instruction of faculty or class instructors. Do not re-enter a building unless given instructions by the following: Austin Fire Department, UT Austin Police Department, or Fire Prevention Services.

* [Information regarding emergency evacuation routes and emergency procedures](http://www.utexas.edu/emergency).

# Sanger Learning Center

More students use the Sanger Learning Center each year to improve their academic performance. All students are welcome to join their classes and workshops and make appointments for their private learning specialists, peer academic coaches, and tutors. For more information, see the [Sanger Web site](http://www.utexas.edu/ugs/slc) or call 512-471-3614 (JES A332).

# Title IX Reporting

Title IX is a federal law that protects against sex and gender-based discrimination, sexual harassment, sexual assault, sexual misconduct, dating/domestic violence and stalking at federally funded educational institutions. UT Austin is committed to fostering a learning and working environment free from discrimination in all its forms where all students, faculty, and staff can learn, work, and thrive. When sexual misconduct occurs in our community, the university can:

1. Intervene to prevent harmful behavior from continuing or escalating.
2. Provide support and remedies to students and employees who have experienced harm or have become involved in a Title IX investigation.
3. Investigate and discipline violations of the university's relevant policies.

Faculty members and certain staff members are considered ``Responsible Employees'' or ``Mandatory Reporters,'' which means that they are required to report violations of Title IX to the Title IX Coordinator at UT Austin. **I am a Responsible Employee and must report any Title IX related incidents** that are disclosed in writing, discussion, or one-on-one. Before talking with me, or with any faculty or staff member about a Title IX related incident, be sure to ask whether they are a responsible employee. If you want to speak with someone for support or remedies without making an official report to the university, email [advocate@austin.utexas.edu](mailto:advocate@austin.utexas.edu). For more info about reporting options and resources, visit [the campus resources page](https://titleix.utexas.edu/campus-resources) or e-mail the Title IX Office at [titleix@austin.utexas.edu](mailto:titleix@austin.utexas.edu).

# Campus Carry

``The University of Texas at Austin is committed to providing a safe environment for students, employees, university affiliates, and visitors, and to respecting the right of individuals who are licensed to carry a handgun as permitted by Texas state law.'' [More information](http://campuscarry.utexas.edu/students).