The University of Texas at Austin
Master of Science in Information Security and Privacy
School of Information and Center for Identity

MSISP 385 (Unique #28520)
Information Risk and Benefit Analysis, Fall 2023

Thompson Conference Center (TCC) Room 3.102, 8 am -12 noon
Instructional Mode: Hybrid

Instructors:

Hüseyin Tanriverdi (email: Huseyin.Tanriverdi@mccombs.utexas.edu; phone: 512-232-9164)
Ashley Hunter (email: Ashley@ahunterco.com; phone: 512-827-9896)
Bruce Kellison (email: bkellison@ic2.utexas.edu; phone: 512-475-7813), Lead Instructor

Office Hours:
Hüseyin Tanriverdi (On Zoom, by appointment)
Ashley Hunter (By appointment)
Bruce Kellison (T, W 4:00 – 5:30 pm or by appointment) Lead Instructor

Office Location:
Hüseyin Tanriverdi (CBA 5.208)
Ashley Hunter (IC^2 Institute, 2815 San Gabriel, Rm 1.114)
Bruce Kellison (IC^2 Institute, 2815 San Gabriel, Rm 1.114) Lead Instructor

Teaching Assistant: Dylan Beldon
E-mail: dylan.beldon@beldon.com
Office Hours: (On Zoom, by appointment)

Course Meeting Dates and Times:

Weekend	Dates	Times	Zoom link
1	August 25-26	8am-12noon	To be posted on Canvas/Zoom folder
2	September 22-23	8am-12noon	To be posted on Canvas/Zoom folder
3	October 13-14	8am-12noon	To be posted on Canvas/Zoom folder
4	November 10-11	8am-12noon	To be posted on Canvas/Zoom folder
5	December 1-2	8am-12noon	To be posted on Canvas/Zoom folder

Course Overview:

Individuals, organizations, and societies invest in digital technologies, big data, and machine learning (ML) and artificial intelligence (AI) algorithms to obtain returns such as efficiency gains, innovations, growth, and profitability. Along with the returns, these technologies can also increase risks of organizations such as privacy risks, information security risks, and risks of unethical, irresponsible use of big data. The objective of this course is to equip students with skills and knowledge for estimating and managing the risks and benefits of these technologies. The course addresses risk/return issues at different levels of analysis such as individuals, organizations, society, and economy.

Course Learning Goals:

By the end of sessions 1-4, students will learn how to estimate the business value of a cybersecurity and privacy investment and communicate it to decision makers in financial terms

- How to estimate total cost of ownership (TCO) of cybersecurity and privacy investment
- How to estimate return on investment (ROI) of cybersecurity and privacy investment
- How to estimate net present value (NPV) of cybersecurity and privacy investment
- How to do "what if" scenario analyses to assess the sensitivity of NPV of cybersecurity and privacy investment to uncertain parameters
- How to quantify cyber loss (CLE) exposure of the investing organization in financial terms
- How to complement the TCO, ROI, NPV, CLE metrics with qualitative arguments to justify the business case of cybersecurity and privacy investment to decision makers

By the end of sessions 5-8, students will:

- Have a working knowledge of cyber liability and supportive insurance forms.
- Understand the differences between traditional risk transfer and alternative risk models and how to apply those models based on the organization's exposures.
- Understand the exposures that are of interest for cyber underwriters and how organizations can implement tools that provide favorable underwriting terms.
- Use reinsurance and financial models to determine underwriting premiums and rates.

By the end of sessions 9 and 10, students will:

- Understand factors that affect national economic efficiency
- Be able to describe assumptions about private economics in a public economy
- Be able to outline national productivity gains from a functioning digital economy that depends on information security and privacy guardrails
- Understand the national security implications of investments in information security related to:
    a) Office of Personnel Management
    b) Transnational/state-sponsored threats: terrorism, cyber war (N. Korea, China, Russia)
    c) International gangs and organized crime syndicates (human trafficking, cyber attacks, Big Data)

Beyond this Course:

The MSISP curriculum prepares students to mitigate information security and privacy risks that threaten the achievement of an organization's business value / public value objectives. Cybersecurity and privacy professionals compete for scarce investment resources of organizations to institute and operate mitigations for cybersecurity and privacy risks. Among the many investment proposals of different business units promising to improve profitability, growth, productivity, etc., why should decision makers fund an information security / privacy investment proposal? This course aims to equip students with skills to estimate risks and benefits of information security / privacy investments so that decision makers can clearly see the business value / public value of the investment and fund the proposal.

Grading policy:

Sessions 1-4: Business value of a cybersecurity and privacy investment (40%)

- Attendance and participation: 2% per session, total of 4x2%=8%
- Session 1 (August 25): HealthCo Case Assignment – Part I (6%)
- Session 2 (August 26): HealthCo Case Assignment – Part II (6%)
- Session 3 (September 22): HealthCo Case Assignment – Part III (10%)
- Session 4 (September 23) HealthCo Case Assignment – Part IV (10%)

Group versus Individual Work for HealthCo Assignments: By default, HealthCo is designed as a group assignment. Please sign up for a 3-person group on Canvas\People\HealthCo Group folder. You have the option to sign up to do the HealthCo assignments on your own if you alert the instructor (Huseyin Tanriverdi) and the TA about it by 8am on July 25th.

Basic Excel skills are required. We will build on the basic Excel functions in doing business value quantification. We will also use a more advanced Excel add-in called @RISK to run Monte Carlo simulations. If your Excel skills are weak, try to form a group with peers who have intermediate or advanced Excel skills. Also, start working on HealthCo assignment early, and learn basic Excel skills on your own.

Windows OS Requirement: The Excel add-in @RISK that we will use for HealthCo assignments is available for Windows OS only. If you have Mac or other operating system, the only way to run @RISK is through a virtual machine installation. In the past, some students used virtual machines without problems, but others ran into problems. To minimize the problems, instructor recommends using a laptop that runs on Windows OS.

Late-submission policy for sessions 1-4: There will be no make-up for missing the assignments of sessions 1-4. If you have to miss an assignment deadline, we would encourage you to do a late submission rather than no submission at all. We will accept a late submission within 7 days after a submission deadline with a penalty. Since solutions will have been presented and discussed in

class on the due dates, late submissions have the benefits of having seen the potential solutions, and hence, a late submission penalty of 20% will be applied.

Sessions 5-8, "Financial Implications of Insuring Information Security Risk"
Students will be provided two case studies surrounding global cyber risks. The students will need to demonstrate understanding of the cyber risks and how to best articulate the exposure in written form for a senior cyber underwriter. The students will be provided with 5 questions for each case study. The final product should at least 6 pages, but no longer than 8 pages for each case study.

Assignment total value: 40%
Assignment Due Date: Nov. 13, 2023, 5:00 pm CST
Late assignment penalty: Late assignment penalty: There is no make-up for missing the assignments. A late submission is better than no submission at all. If you miss the submission deadline, a late submission within 7 days after the submission deadline will be accepted with a penalty. Since we will have discussed the assignments in class on the due dates, late submissions will have the benefit of that discussion, and hence, they will be subject to a late submission penalty of 20% reduction.

Sessions 9 and 10, "Societal Impacts of Identity Assets"
Individual assignment: Create a hypothetical public organization, national in scope, and describe its role and function. Create identity assets for your organization. Describe how you value them, and why they should be protected. Describe your organization's position vis-à-vis other federal agencies. Does it share information with other agencies? What identity protection investments should your organization make in the short, medium, and long term?

Assignment total value: 20%
Assignment Due Date: Dec. 5, 5:00 pm CST
Late assignment penalty: There is no make-up for missing the assignments. A late submission is better than no submission at all. If you miss the submission deadline, a late submission within 7 days after the submission deadline will be accepted with a penalty. Since we will have discussed the assignments in class on the due dates, late submissions will have the benefit of that discussion, and hence, they will be subject to a late submission penalty of 20% reduction.

University of Texas and MSISP grading policies

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 they will 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.

Final course letter grades: The weighted average of the grade components will be used to assign final letter grades. The following table is used to convert weighted grade averages to final letter grades. No rounding will be applied.

The instructor reserves the right to adjust numeric ranges, provided all adjustments are made fairly and uniformly for the entire class and to the benefit of the students. For example, if the class average turns out to be lower than anticipated, the instructor can choose to shift down the numeric ranges of letter grades.

Weighted average of grade components	Letter grade category
90-100	A
80-89.99	B
70-79.99	C
60-69.99	D
00-59.99	F

Attendance and participation in class are an important part of the success of our course and will be considered part of the course grade at the instructors' discretion. Please understand the hybrid nature of the course means that we will make video recordings of our class sessions available on Canvas, watching video recordings are not a replacement for attendance.

Excused Absences
Attendance is mandatory for all MSISP classes. Students must attend classes in-person or remotely via Zoom. While class lectures are recorded in support of students' studies, review of class recordings does not constitute attendance. Only extraordinary, documented requests submitted at least 72 hours in advance of class time will be considered for absences. There must be a compelling reason for any requests not submitted 72 hours in advance of class start. Acceptance of excused absences will be considered by the faculty instructor in consultation with the MSISP Program Director.

Schedule

Session # (Date)	Main Topic(s)	Instructor or Guest Lecturer
1 (8/25)	**Total cost of ownership (TCO) and return on investment (ROI) of cybersecurity and privacy investments** • (Canvas) Sotnikov, I. (2023). "ROI For Cybersecurity: How To Position Security Solutions As Investments" Forbes Technology Council. • (Canvas) O'Niell, C., Khurana, V., Troha, C., Holstege, B., Bartol, N., Asen, A., Cheung, G., Fallon, M., and Gapp, B. (2023). "As Budgets Get Tighter, Cybersecurity Must Get Smarter" Boston Consulting Group's Annual Cybersecurity Survey 2023.	Hüseyin Tanriverdi

	• (Canvas). Technology Finance Partners. (2019). "Total cost of ownership (TCO) versus Return on investment (ROI): Which is Best for Making Investment Decisions?" • (Canvas) HealthCo Case Assignment and Excel Workbook– See Part I.	
2 (8/26)	**Net present value (NPV) of cybersecurity and privacy investments** • (Canvas) Girardin, M. (2023). "How to Calculate Net Present Value (NPV)." • (Canvas). Moore, M.H., and Khagram, S. (2004). "On creating public value: what business might learn from government about strategic management," Corporate Social Responsibility Initiative Working Paper #3, Cambridge, MA: John F. Kennedy School of Government, Harvard University. • Prepare to learn and apply @RISK tools ▪ Download and install @RISK tools of Palisade (now Lumivero) ▪ @RISK Guided Tour - Basic Features - Sensitivity Analysis https://www.youtube.com/watch?v=TT10GJ0nTKE ▪ Learn basic functionality of @RISK: https://www.palisade.com/videos/ • (Canvas). HealthCo Case Assignment and Excel Workbook– See Part II.	Hüseyin Tanriverdi
3 (9/22)	**Sensitivity analysis with Monte Carlo simulations** • Prepare to learn and apply @RISK tools ▪ Download and install @RISK tools of Palisade (now Lumivero) ▪ @RISK Guided Tour - Basic Features - Sensitivity Analysis https://www.youtube.com/watch?v=TT10GJ0nTKE ▪ Learn basic functionality of @RISK: https://www.palisade.com/videos/ ▪ For additional guidance and tutorials on @RISK tools, see YouTube channel of @RISK: https://www.youtube.com/@RISKbyLumivero/videos • (Canvas). HealthCo Case Assignment and Excel Workbook– See Part III.	Hüseyin Tanriverdi
4 (9/23)	**Estimating cyber loss exposure** • (Canvas) Jones, J. (2023). "Today's Cyber Risk Measurement Best Practices." FAIR Institute. • (Canvas) Martin-Vegue, T. (2021). "The Elephant in the Risk Governance Room." ISACA. • Sign up for a free FAIR-U account (https://www.fairinstitute.org/fair-u), do the sample	Hüseyin Tanriverdi

	exercise in preparation for applying this risk quantification tool HealthCo case. • (Canvas). HealthCo Case Assignment and Excel Workbook– See Part IV. • At Dr. Suzanne Barber's request, this session will end at 11am to allow students to participate in a panel discussion by the UT-CID's Advisory Board. Dr. Barber will share the details.	
5 (10/13)	**Fundamentals of Professional and General Liability Insurance** (Canvas) 2022 Ponemon Institute: Keeper Report **Professional Liability (Cyber and Technology Risk) Overview**	Ashley M. Hunter
6 (10/14)	**Financial Analysis** **Professional Liability Reinsurance** (Canvas) 2022 Verizon: Data Breach Investigations Report **Alternative Risk Markets** **Privacy and Data Security Liability**	Ashley M. Hunter
7 (11/10)	**Privacy and Data Security Liability *(cont.)*** **Reinsurance** (Canvas) "The Steps CIOs Must Take To Deal With Ransomware Attacks Like The One That Hit Garmin*"* (2020, Forbes) **Insurer Financial Statements**	Ashley M. Hunter
8 (11/11)	**Interpreting Insurer Financial Statements** **Insurer Financial Management** (Canvas) "What Is the Real Cost of a Data Breach? New Report Indicates It's About $4 Million to $9 Million for SMEs" (2020, CPO Magazine) **Insurer Strategic Management and Global Operations**	Ashley M. Hunter
9 (12/1)	**Elements of national macroeconomic efficiency** **Assumptions about private economics in a public economy** **Productivity and Privacy: Healthcare** (Canvas) Parks, Wigand, and Lowry, "Balancing information privacy and operational utility in healthcare: proposing a privacy impact assessment (PIA) framework," (2022); and selected chapters from Camp & Johnson (2012). *The Economics of Financial and Medical Identity Theft*	Bruce Kellison
10 (12/2)	**Issues of national security: IRS, OPM breaches** **Issues of national security: State-sponsored threats**	Bruce Kellison

	Issues of national security: international organized crime (Canvas) Wehbé, "OPM Data Breach Case Study: Mitigating Personnel Security Risk" (2017) Seeley, "Once More Unto the Breach: The Constitutional Right to Informational Privacy and the Privacy Act" (2016)	

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 Professor Kellison, as Lead Instructor, know as soon as possible. Together we will develop strategies to meet your needs and the course requirements. We 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.

Acceptable Use of ChatGPT and Similar AI Tools in Assignments

The University has developed an acceptable use policy for ChatGPT and other AI tools. It is available here: https://security.utexas.edu/ai-tools.

In this course, students may use AI tools for assignment preparation **if they disclose which AI tool they used for what aspects of an assignment**. Furthermore, students must understand and acknowledge that they are accountable for the authenticity and integrity of the assignments they turn in, including proper citation, attribution, and accuracy of the sources used in the assignment.

Use of Electronics

To help you connect the pieces of the class together, please focus the use of electronics on the content in lecture and laboratory.

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 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 Professor Kellison 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 (SSD). Here are some examples of the types of diagnoses and conditions that can be considered disabilities: Attention-Deficit/Hyperactivity Disorders (ADHD), Autism, Blind & Visually Impaired, Brain Injuries, Deaf & Hard of Hearing, Learning Disabilities, Medical Disabilities, Physical Disabilities, Psychological Disabilities and Temporary Disabilities. Please refer to SSD's website for contact and more information. If you are already registered with SSD, please deliver your Accommodation Letter to Professor Kellison as early as possible in the semester so we can discuss your approved accommodations and needs in this course.

Mental Health Counseling

College 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 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. 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 and University policies on class 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. 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 and University policies on class 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.

COVID-19 Guidance

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

- Adhere to university mask guidance.
- Vaccinations are widely available, 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 remains an important part of the university's efforts to protect our community. Tests are fast and free.
- Visit Protect Texas Together 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 Behavioral 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 the lead 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.

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 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. All three of your course instructors are **Responsible Employees and must report any Title IX related incidents** that are disclosed in writing, discussion, or one-on-one. Before talking with us, 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. For more info about reporting options and resources, visit the campus resources page or e-mail the Title IX Office at 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.