Cybersecurity Fundamentals Course Syllabus

Updated Materials: Technology, audit, engineering, or military (any discipline) Background Strongly Recommended. Contact me if you are uncertain.

Course Title: **Cybersecurity Fundamentals**

Class Info.:

Class Section:	MIS6311.501.16F	**Activity Type:**	Lecture
Class Level:	Graduate	**Class Number:**	83732
Class Credits:	3.00 Credits	**Inst. Mode:**	Face-to-Face
Grading:	Graded - Graduate	**Session Type:**	Regular Academic Session (1)

Status: **Section Status:** OPEN **Available Seats:** 4 **Enrolled Total:** 56 **Waitlist:** 0

Description: **MIS 6311** - **Cybersecurity Fundamentals** (3 semester credit hours) The course provides an overview of various technical and managerial issues associated with cybersecurity. The topics include risk assessment and management, cybersecurity programs, IT security controls and technologies, security standards and laws, IT auditing, cyber insurance, and other cyber risk mitigation strategies. (3-0) S

Instructor(s): Christopher Davis **email:** cmd140430@utdallas.edu

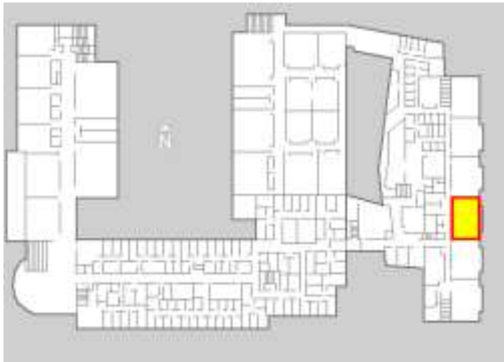
Class Location and Times

Location: UT Dallas - Main Campus

Monday: 7:00pm-9:45pm JSOM 12.210

Term: Fall 2016
Session Type: Regular Academic Session (1)
Starts: August 22, 2016
Ends: December 15, 2016

Schedule: JSOM Building - Floor 2 - Room 12.210



Cross Listed With: MIS6311.501.16F - Cybersecurity Fundamentals
ACCT6312.501.16F - Cybersecurity Fundamentals

College: Jindal School of Management

Professor Contact Information

Chris Davis
Google Voice: 214-771-8122
UTD Email: cmd140430@utdallas.edu
LinkedIn: www.LinkedIn.com/in/ChristopherDavis
Blog: www.cloudauditcontrols.com

Course Pre-requisites, Co-requisites, and/or Other Restrictions

Updated Materials: Technology, audit, engineering, or military (any discipline) Background Strongly Recommended. Contact me if you are uncertain.

Course Description

MIS 6311 - Cybersecurity Fundamentals (3 semester credit hours) The course provides an overview of building and breaking the fundamentals of cyber security based on the principles behind the coveted Certified Information Systems Security Professional (CISSP). Topics include access controls, telecommunications and network security, risk management, software development security, cryptography, security architecture and design, operations security, business continuity, regulations, investigations, forensics, compliance, physical security, and emerging technologies. Please see the session break out for additional information. (3-0) S

Student Learning Objectives/Outcomes

Very simply, in plain English, students of this course acquire practical knowledge that forms the foundation for additional studies in a variety of information security disciplines. This is a graduate level course, and many of the students are working professionals – as is the instructor. You can apply this knowledge directly and indirectly to your company projects.

Required Textbooks and Materials

- CISSP All-In-One Exam Guide: http://www.amazon.com/dp/0071781749/

What version of the text you buy, whether hardcover or Kindle edition, is completely up to you. Highly recommend the exam questions if this is a professional certification that you would be interested in taking in the future.

Optional Course Materials

- *IT Auditing, Using Controls to Protect Information Assets,* Davis, Schiller, McGraw-Hill, 2010 – Some of the materials and perspectives will come from this book.
- *http://www.sans.org/reading-room/*

Assignments & Academic Calendar

Academic calendar: https://www.utdallas.edu/academiccalendar
Class link: http://coursebook.utdallas.edu/mis6311.501

Class sessions will cover the following:

	Topics	Ch.	General Comments
1	Course Overview; GRC and IT Controls; Building the Security Program	**Class**	**Plan. Execute with purpose.** We are going to build effective security programs. Only the best programs make it. **Design. Architect genius.** Starting with our requirements, we are going to build a robust security program. Here's how to be successful and avoid the pitfalls that get organizations into trouble.
2	Access Control	**3**	**Actor control point.** Collection of mechanisms that work together to create security architecture to protect the assets of the information system.
3	Telecommunications and Network Security	**6**	**Communications control point.** Discusses network structures, transmission methods, transport formats and security measures used to provide availability, integrity and confidentiality.
4	Information Security Governance and Risk Management	**2**	**Systems perspectives.** The identification of an organization's information assets and the development, documentation and implementation of policies, standards, procedures and guidelines.
5	Software Development Security	**10**	**Before the fight.** Refers to the controls that are included within systems and applications software and the steps used in their development
6	Cryptography	**7**	**Spies and Lies.** The principles, means and methods of disguising information to ensure its integrity, confidentiality and authenticity.
7	Operations Security	**4**	**Principled genius.** Contains the concepts, principles, structures and standards used to design, implement, monitor, and secure, operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity and availability.
8	Security Architecture and Design	**11**	**Objective execution.** Used to identify the controls over hardware, media and the operators with access privileges to any of these resources.
9	Business Continuity and Disaster Recovery Planning	**8**	**Objective recovery.** Addresses the preservation of the business in the face of major disruptions to normal business operations.
10	Legal, Regulations, Investigations and	**9**	**Objective response.** Addresses computer crime laws and regulations; the investigative measures and techniques which can be used to determine if

	Forensics		a crime has been committed and methods to gather evidence.
11	Physical (Environmental) Security	**5**	**Physical control point.** Addresses the threats, vulnerabilities and countermeasures that can physically protect an enterprise’s resources and sensitive information.

12	Emerging Technologies;
	The Reality of Soft Skills;
	Compromising Security Programs
		Class	**Agility and applications.** Technology changes quickly, which changes vulnerability profiles and attack vectors. Let's review the latest technologies and apply what we've learned so that you know how to assess this changing landscape and apply your knowledge to real-world scenarios. Never be caught off guard without a plan to get an answer.;
			Skilled Delivery. The success of your security program depends on more than technology. It’s your soft skills. Let’s examine the reality of positioning, selling, politics, and communications as it relates to security. And the best part - these skills make you more effective professionally, and more well-rounded personally.;
			We've built it. Now let's break it. Learn ages old methodologies for compromising security programs. Logical. Physical. Social.

13	Personal Recommendations [Floating Week]	**Class**	**Practical Applications.** Addresses the threats and vulnerabilities that can affect your personal resources and sensitive information. Review countermeasures that can protect them. [Class can be used to bring in guest speakers, address other topics based on class interest.]
	[Presentations]		[Team Presentations]
	[Final]		[Final]

Grading Policy & Course Requirements

Course Requirements Summary:		
Category	**Weight**	**Comments**
Class Participation	**25%**	Class Assignments and Participation
Project	**25%**	Students may choose one of the following options: 1. Subject Area Analysis 2. Data Breach Analysis 3. Risk and Controls Analysis
Exam 1	**20%**	Midterm Exam
Exam 2	**30%**	Final Exam

Project Selection

The focus in this course is on learning how to build the information technology control underpinnings of an effective security and risk management program. My goal is always to dive deeper into the information and we are just scraping the surface. Use the projects as an opportunity to learn and stretch the bounds of your understanding.

Class members have the option to prepare each case write-up on an individual basis or as a group. There is a benefit to both. Groups get to share the load, but are required to share their findings with the class in a 10 to 15 minute presentation.

Individuals completing the project alone are not required to deliver a presentation to the class. However, many have chosen to share their research and you are more than welcome to do so.

All students must choose one of the following three options for their write-up:

1. **Course Subject Area Analysis**

   Prepare and deliver an analysis of a relevant topic or subject area germane to the course. Topics may be chosen from any class session content description in the syllabus. The purpose of this analysis is to dive deeper into a subject area, learn the material, and share your findings with the class.

   – OR –

2. **Data Breach Analysis**

   Analyze risks and control failures that led to a known data breach from those listed on www.privacyrights.org/ar/ChronDataBreaches.htm. Details should include a descriptive chronology of what happened and how effective security and risk management programs could have been effective in mitigating the risk that led to the breach.

   – OR –

3. **Risk and Controls Analysis**

   Students will demonstrate understanding and analysis capabilities by choosing either a subject area, technology, or a designated system to detail actual or typical implemented controls and residual risk. The purpose of this analysis is to demonstrate conceptual familiarity and practical application of risks and controls.

Project Requirements

Class members have the option to prepare each case write-up on an individual basis or as a group project write-up. The project may be completed with teams up to three people. No exceptions. Here are the general requirements for each write-up:

1. **Format:** The concise written overview should be approximately 4-5 pages in length. If needed, you can exceed 5 pages as long as the writing is concise and well focused. Quality > Quantity. Do not double-space. We are not in elementary school.
2. **Production Units:** One electronic or paper copy per self-selected team.
3. **Presentation (Groups Only)**: Individuals completing the project alone are not required to deliver a presentation. Certainly, you may, and other people will benefit from your findings. Project teams will be required to deliver a 10-15 minute overview of what they studied. These presentations tend to be a lot of fun.

Project Grading

- **A - Professional-level communication**. If you were applying for a job that specified "excellent communications skills," you could submit this paper as a writing sample. The tone is businesslike, courteous, and confident. The structure demonstrates an understanding of the professional genre. An A paper goes beyond fulfilling the assignment's requirements, demonstrating superior skills in conveying information both verbally and visually.
- **B - Competent work**. This level of writing shows that you have followed the instructions and given a clear, complete explanation or description with no major errors in formatting or use of language. The material meets the assignment's requirements, but demonstrates no significant effort to facilitate the reader's comprehension. A B paper is well done, but it is unmistakably undergraduate level work.
- **C - Assignment completed without distinction**. This level of writing shows that you have done the assignment, but the reader has to work to understand it. A C paper is notably lacking in attention to detail, usually indicating a need for revision and remedial help; occasionally, however, a well-written paper may receive a C for violating significant conventions of professional writing, such as using a tone that might offend some readers, violation of professional writing conventions (such as consistent use of non-standard vocabulary or punctuation), or egregious errors in formatting or presentation.
- **D - Has not fulfilled the assignment and will not pass without significant revision.**
- **F - Indicates complete lack of effort, plagiarism, or some other violation of Institute requirements.**

Mid-Term and Final Exams

1. The essay exam covers material from class sessions.
2. The purpose of this course is to develop an **understanding** of the theory and application of effective security and risk management (rather than memorization of lists or diagrams). Given this course philosophy, you may develop a resource binder of class lecture notes, articles, book chapter **summaries,** your personal notes, and minor reproduction of book charts for use during the exam. The exams are **open book**. And open Internet. I depend upon Google at work, and I'm sure you do as well.

Course & Instructor Policies

We are all adults in this class, with busy schedules. If you have questions or concerns, I expect you to take the initiative and bring your concerns up with me.

1. Makeup exams: If you have an extraordinary situation requiring a makeup exam, please discuss early.
2. Extra credit: This course does not have extra credit. The requirements of the course are extremely simple. Do well on your project, midterm, and final exam. Attend class.
3. Late work: Late work is not applicable for this course. Projects turned in after the final day of classes will generally not be accepted.
4. Class attendance: You are expected to attend class. Please do not sign up for this class if you do not intend on being there. Sessions at UTD are not recorded.
5. Classroom citizenship: Please conduct yourself in a manner conducive to learning in a classroom environment.

   You must earn above a 90% for an A, 80% for a B, 70% for a C and less than 70% is a failing grade. Grades of +'s will be given.

UT Dallas Syllabus Policies and Procedures

The information contained in the following link constitutes the University's policies and procedures segment of the course syllabus.

Please go to http://go.utdallas.edu/syllabus-policies for these policies.

The descriptions and timelines contained in this syllabus are subject to change at the discretion of the Professor.