MARYMOUNT UNIVERSITY

School of Business Administration
2017-18 Fall Semester

COURSE SYLLABUS

Course Number IT-530-A	**Course Title** COMPUTER SECURITY		
Fall Semester XXX	**Spring Semester**	**Summer Semester**	**Credit Hours** 3
Name of Instructor: Dr. Ibrahim Waziri, Jr.			
Meeting Day, Time, and Room Number 8/30/17 – 12/16/17, Wed, 6:30pm – 9:15pm, Room: Ballston 3046			
Office Hours, Location, Phone: Available by e-mail or appointment as needed			
E-mail: iwaziri@marymount.edu **Class webpage:** iiwaziri.com/Fall17IT530A.html			

UNIVERSITY STATEMENTS

Academic Integrity

By accepting this syllabus, you pledge to uphold the principles of Academic Integrity expressed by the Marymount University Community. You agree to observe these principles yourself and to defend them against abuse by others.

Special Needs and Accommodations

Please advise the instructor of any special concerns or needs at the beginning of the semester. If you seek accommodation based on disabilities, you should provide a Faculty Contact Sheet obtained through the Office of Student Access Services, located in Rowley Hall.

Access to Student Work

Copies of your work in this course including copies of any submitted papers and your portfolios may be kept on file for institutional research, assessment and accreditation purposes. All work used for these purposes will be submitted anonymously.

Student Copyright Authorization

For the benefit of current and future students, work in this course may be used for educational critique, demonstrations, samples, presentations, and verification. Outside of these uses, work shall not be sold, copied, broadcast, or distributed for profit without student consent. Items submitted for this course also may be submitted to TurnItIn.com for analysis.

University Policy on Weather and Emergency Closings

Weather and Emergency closings are announced on Marymount's web site, through MUAlerts, area radio stations, and TV stations. You may also call the Weather and Emergency Hotline at (703) 526-6888 for current status. Unless otherwise advised by local media or by official bulletins listed above, students are expected to report for class as near normal time as possible on days when weather conditions are adverse. Decisions as to inclement closing or delayed opening are not generally made before 6:00 AM and by 3:00 PM for evening classes of the working day. Emergency closing could occur at any time making MUAlerts the timeliest announcement mechanism. Students are expected to attend class if the University is not officially closed. If the University is closed, course content and assignments will still be covered as directed by the course instructor. Please look for communication from course instructor (e.g., Blackboard) for information on course work during periods in which the University is closed.

1. BROAD PURPOSE OF COURSE

This course provides an overview for the computer security risks facing enterprises today and covers the many options available for mitigation of these risks. Topics include security concepts, controls, and techniques; standards; designing, monitoring, and securing operating systems; hardware; applications; databases; networks (wired and wireless); and the controls used to enforce various levels of availability, confidentiality and integrity. Computer security is taught in the context of the increasingly global and distributed environment of today's enterprise. Business continuity and disaster recovery planning are also discussed. Prerequisite: IT 520. (3)

2. COURSE OBJECTIVES: Upon successful completion of this course students will be expected to:

a. Explain the goals of computer security and distinguish between common computer security terms;
b. Explain the issues of computer privacy including identity theft;
c. Classify the major threats to computer systems and describe the typical countermeasures;
d. Examine the technological, social, legal, and ethical dimensions of computer security;
e. Make computer security decisions with consideration of their technical, social, legal, and ethical context;
f. Independently research computer security incidents and evaluate them from their technological, social, legal, and ethical perspectives;
g. Evaluate security and privacy policies; and
h. Examine the personnel requirements for an information security office, including researching available certifications.

Specific topic coverage includes:

- Introduction to Information Security
- The Need for Security
- Legal, Ethical, and Professional Issues in Information Security
- Planning for Security
- Risk Management
- Security Technology: Firewalls, VPNs, and Wireless
- Security Technology: Intrusion Detection and Prevention Systems and Other Security Tools
- Cryptography
- Physical Security
- Implementing Information Security
- Security and Personnel
- Information Security Maintenance and eDiscovery

3. TEACHING METHOD

This class will cover a wide array of topics through various methods of instruction; Lectures on material, tool demonstrations, group discussions, and open forums. Classes will be instructor led, but student driven – student participation and interaction is required for this course. Assignments throughout the semester are geared towards making the student think critically on the subject matter, learn the aspects of information security, and implement knowledge gained as a security professional.

4. GRADING POLICY

The course will follow the scoring table listed below: All grades will be on Canvas

Category:	*Grade Percentage*
Proposal & Response	20%
Assignments (10)	30%
Research Paper	25%
Presentation 1 (Midterm)	10%
Final Exam	15%
Total:	100%

Percentage:	*Letter Grade*
90-100%	A
80-89%	B
70-79%	C
60-69%	D
0-59%	F

Proposal & Response: Starting second week of classes. One student per week will be proposing a solution to any current cybersecurity problem. This proposal will be followed by a response from another student that offers a helpful critique. The proposal in class should be preceded by a brief paper (2-3 page including bibliographic references.) that will be distributed to the remainder of the class and to me (via email) by 2:00pm the day before our class session. The respondent will prepare a 1-page (no need for bibliographic references) response to that paper. The respondent should have a draft of the reporter's paper no later than 12:00pm the day before we meet. The main report will be orally presented in class (visuals, i.e.: PowerPoint are a good idea, but not required). The respondent will respond (which I guess is what respondents do). The response paper should be distributed to the class and to me (via email) no later than 12:00pm of the day we meet. Discussion from classmates should ensue from these reports indicating that everyone is prepared to respond to the readings. Altogether, these activities – proposals, responses, and participation in the class constitute 20% of your grade. It should go without saying that all class discussion should be done in a civil, but not uncritical, manner.

Assignments: There will be ten (10) assignments provided throughout the semester, one per lecture. (Available on the class web page) The questions will largely be open response but may also include multiple choice, essays, or fill in the blank. The content of each assignment will be focused on its corresponding lecture. All assignments are to be handed in at the BEGINNING of the class period, in the classroom, on the specified due date unless states otherwise. Assignments constitute 30% of your grade. Late assignments will NOT be accepted and will receive an automatic zero. Exceptions to this policy will only be made in the event of a medical emergency and advanced notification. However, extra credit assignments will be provided as an opportunity to replace up to two (2) missed assignments.

Research Paper: Students will be expected to write one research paper suitable for publication in a peer-reviewed publication. The paper will be 7,000 to 8,000 words minus data presentations and bibliographic references. You may choose a topic that attempts to provide a Technology/Information Security solution to any of the 17 SDGs. Carefully construct a set of questions related to the issue. Conduct your own literature review of the issue. Write up your results in the form of a report that includes an introduction describing the issue in depth, a review of the literature related to the issue, and an analysis and your findings. This paper must be submitted as a full paper, on its due date and with a minimum of 12 references. I will ask you to provide a one-page summary of what you think you wish to do by Sept 13th 2017. You may seek my permission to change subjects if you think your initial issues are leading you to a dead end. However, changing subject will not provide you with an additional time, or changes to an already graded submission. Research Paper constitute 25% of your grade.

Presentation: Students will make 2 presentations for the research paper:

Presentation 1: The first presentation (10-15 minutes), will outline the issue and the interface; This will be supported by a relatively short introduction, literature search and analysis approach. This presentation needs to have at least 6-7 references. This allows me to see what direction your paper is going. This presentation will serve as midterm.

Presentation 2: Students will make a final presentation of the full paper at the end of the course. This presentation should last at least 30 minutes. The grade for this presentation part of 25% grade of the research paper

Final Exam: The final exam will be based on the textbook and assignments. Students will have the full class (2 hours 45 minutes) to complete the exam.

5. CLASS SCHEDULE

The weekly coverage might change as it depends on the progress of the class. However, you must keep up with the reading assignments.

Date	Topics	Due
30 Aug 17 **Week1**	Introduction – Review of Syllabus Chapter 1: Introduction to Information Security History & Definition of Information Security NSTISSC Security Model, ISO 27001 ISMS, CoBIT, NIST 800-53, NIST CSF Critical Characteristics of Information Information Security Models Balancing Security and Access Security SDLC Communities of Interest Assignment 1	
06 Sept 17 **Week2**	Chapter 2: The Need for Security Review of Security Incidents Business vs Technology Threats to and Vulnerabilities of Systems Known Attacks Malicious Code Denial-of-Service Spoofing Social Engineering Assignment 2	Assignment 1 due before class Proposal & Critique
13 Sept 17 **Week3**	Chapter 3: Legal, Ethical, and Professional Issues in Information Security Laws and Regulations Related to InfoSec Ethical Issues in InfoSec Operations Legal Elements (investigative authorities) Types of Law Relevant U.S. laws Policy vs Law & International Laws Codes of Ethics Need for Legal Counsel Assignment 3	Assignment 2 due before class Research Topics Due (Abstract/Framework) Proposal & Critique

20 Sept 17 **Week4**	Chapter 5: Risk Management Risk Identification Threat/Vulnerability Assessment Cost/Benefit Analysis Risk Mitigation (implementing and maintaining) Chapter 6: Security Technology: Firewalls and VPNs Authentication Access Control Firewall types and operations Remote access Virtual private networks Other Topics: CVSS Model 3, STRIDE / DREAD Assignment 4	Assignment 3 due before class Proposal & Critique
27 Sept 17 **Week5**	Chapter 7: Security Technology: IDS & Prevention Systems Intrusion Detection and Access Control Techniques Intrusion Detection Systems Intrusion Prevention Systems Honeypots and Honeynets Access Control Techniques Biometrics Assignment 5 Research Topics Feedback (Last 1hr of class)	Assignment 4 due before class Proposal & Critique
04 Oct **Week6**	Chapter 4: Planning for Security Security planning Security Policy Project management Incident response Business Continuity Planning Disaster Recovery Incident Response Contingency Planning	Assignment 5 due before class Proposal & Critique
11 Oct **Week 7**	Presentations 1 - Research Progress (Midterm) Assignment 6	
18 Oct 17 **Week8**	Chapter 8: Cryptography Encryption and Decryption Poly-alphabetic ciphers History of Cryptology Symmetric Ciphers Public Key Systems (RSA) Hash functions (SHA, MD5) Cryptographic Applications Protocols (SSL/TSL) Digital signatures and certificates Assignment 7	Assignment 6 due before class Proposal & Critique
25 Oct 17 **Week9**	Chapter 9: Physical Security Physical access control (locks, cards) Fire safety methods Building construction Power controls (ups, etc) Environmental controls (HVAC, etc) Assignment 8	Assignment 7 due before class Proposal & Critique
01 Nov 17 **Week10**	Chapter 10: Implementing Information Security Information Security Project Management Technical Aspects of Implementation Non-Technical Aspects of Implementation Information Systems Security Certification & Accreditation	Assignment 8 due before class Proposal & Critique

	Assignment 9	
08 Nov 17 **Week11**	Chapter 11: Security & Personnel Personnel Security Practices and Procedures Authentication and Authorization Security Training Security Awareness Training Need-to-know, Rotation and Minimal Access Principles Background Checks Clearances Assignment 10 Assignment: Extra Credit	Assignment 9 due before class Proposal & Critique
15 Nov 17 **Week12**	Chapter 12: Information Security Maintenance Maintaining a Secure Environment Maintenance Model Configuration Management Change management Updates, patches and fixes Monitoring and auditing System Life Cycle	Assignment 10 due before class Extra Credit Assignment Due Proposal & Critique
22 Nov 17 **Week 13**	Thanksgiving	
29 Nov 17 **Week14**	Final Presentations	Research Papers due before class
06 Dec 17 **Week15**	Final Presentations Lecture: Final Exam Review (Cumulative)	
13 Dec 17 **Week16**	**Final Exam**	**N/A**

6. REQUIRED TEXT

Principles of Information Security, Fifth Edition
Michael E. Whitman and Herbert J. Mattord
ISBN-13: 978-1-285-44836-7
ISBN-10: 1-285-44836-7