MARYMOUNT UNIVERSITY

School of Business and Technology
2019-20

COURSE SYLLABUS

Course Number: IT 737-OL	**Course Title:** Securing the Evolving Technology Infrastructure

Fall Semester	**Spring Semester**	**Summer Semester**	**Credit Hours**
2020		XXX	3

Name of Instructor: Dr. Ibrahim Waziri Jr.

Meeting Day, Time, and Room Number: Fully Online - **Asynchronous**

Final Exam Day, Time, and Room Number: Online

Office Hours, Location, Phone: Online – By Appointment Only (Number is available on Canvas and Kick-Off Deck)

E-mail and Web Site: - Website: Canvas – **Repo:** https://github.com/iwazirijr/IT737

Course Description: This doctoral-level course examines the cybersecurity challenges of the constantly changing computing infrastructure with its increasing reliance on the Internet and the rise of additional threats posed by cloud computing, mobile computing, integration of the Internet of Things, automated industrial control systems, use of hardware built in other countries, and the risk of other critical infrastructures. This course examines the cybersecurity challenges of interrelated systems across the global landscape and the different techniques used to protect computers and data, with particular emphasis on sectors such as transportation, utilities, health care, financial services, and manufacturing.

1. **BROAD PURPOSE OF COURSE:** This course covers the knowledge and skills for the global leadership that is needed to protect and safeguard the broad range of what is considered to be critical infrastructure. It focuses on planning, designing, implementing and managing the protection of today's evolving technology in infrastructure. It will examine the best practices and global standards in ever evolving technology. The course will also provide doctoral students with the needed information to contribute toward society their expert knowledge of protecting global components of evolving infrastructure technology

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

- Know the specific 16 - areas of critical infrastructure as defined by DHS CISA.
- Know the specific countermeasures in protecting against intrusion of defined critical infrastructure.
- Demonstrate the knowledge of detecting security risks and risk awareness of defined global industries and infrastructure.
- Understand the economic impacts and risks of not protecting global infrastructure and industries.
- Explain the integral parts of evolving critical infrastructure technology.
- Describe the various types of plans and steps in developing mitigation strategies for evolving technology infrastructure.
- Evaluate risk management approaches in securing evolving technology infrastructure.
- Identify and describe the various security issues related to evolving technology infrastructure.
- Describe and demonstrate security governance as it relates to protecting infrastructure technology.

3. **TEACHING METHOD:** Because this class is an asynchronous class. Doctoral students will learn by reading research papers, writing reports, watching referenced videos, and writing a final research paper to be submitted to a journal or conference. As your instructor, it is my responsibility to present learning opportunities through the various components outlined in the course syllabus. As the student, it is your responsibility to do the learning by completing the assigned work, by participating in discussions and group activities with energy, enthusiasm and relevant content.

4. **GRADING POLICY**

Grade	Grade Range	Deliverable Grade	% of Final Grade
A	90 – 100%	Topic Summary (10 @ 5% each)	50%
B	80 – 89.9%	Final Research Paper	50%
C	70 – 79.9%		
F	Below 70%	**TOTAL**	**100%**

May 22, 2020 is the last day to add or drop a SU III course without academic record and with a 100% refund
June 19, 2020 is the last day to withdraw from a SU III class with a grade of W

5. **CLASS SCHEDULE**

Week Module	Topics (instructor to deliver)	Task (student to-do)
Week 1 Module - 1 Kick-Off	• Kick-Off: Syllabus Overview and Class Structure • Evolving Technology Infrastructure	• Read/Watch Lecture Materials • Submit Weekly Published Paper Summary • Introduce yourself • **Due Fri 05/22 at 6.30PM**
Week 2 Module 2	• Securing Cloud Computing Infrastructure • DHS CISA TIC (Trusted Internet Connections)	• Read/Watch Lecture Materials • Submit Weekly Published Paper Summary • Identify research paper topic • Upload research paper topic and brief description to Professor for approval • **Due Fri 05/29 at 6.30PM**
Week 3 Module 3	• Securing Internet of Things (IOT)	• Read/Watch Lecture Materials • Submit Weekly Published Paper Summary • Continue working on final research paper • Identify a journal/conference to submit final research paper - Marymount University Library Archives is also an option. • Upload the name and link of identified journal or conference to submit final research paper • **Due Fri 06/05 at 6.30PM**
Week 4 Module 4	• Securing Robotic Process Automations (RPA)	• Read/Watch Lecture Materials • Submit Weekly Published Paper Summary • Continue working on final research paper
Week 5 Module 5	• Securing Artificial Intelligence (AI)	
Week 6 Module 6	• Securing Autonomous Vehicles, Drones and Robots	• Read/Watch Lecture Materials • Submit Weekly Published Paper Summary • Final research paper – Check-in/Progress • Upload research paper progress (optional) • **Due Fri 06/26 at 6.30PM**
Week 7 Module 7	• Securing Mobile Infrastructures (Cell Towers & Scanners)	• Read/Watch Lecture Materials • Submit Weekly Published Paper Summary • Continue working on final research paper
Week 8 Module 8	• Securing National Grids (Electric Grid and Power Plants) and Industrial Control Systems– SCADA	• Read/Watch Lecture Materials • Submit Weekly Published Paper Summary • Final research paper – Check-in/Progress • Upload draft research paper in journal/conference format for professor feedback. • **Due Fri 07/10 at 6.30PM**
Week 9 Module 9	• Securing National Infrastructures (Bridges, Roads) and Transportation (Metro, Rail, Train) Systems by leveraging ISAC	• Read/Watch Lecture Materials • Submit Weekly Published Paper Summary • Continue working on final research paper
Week 10 Module 10	• Infrastructure Information Sharing & Security Operation Centers • U.S. DHS CISA NICC • Intelligence and Information Sharing - FBI Infragard (Infrastructure Protection Program)	• Read/Watch Lecture Materials • Submit Weekly Published Paper Summary • Incorporate feedback and email final version to professor for final approval • **Due Fri 07/24 at 6.30PM**
Week 11 Module 11	**Class ends/everything is due**	• **Upload Final Research Paper and send evidence to professor** • **Due: Friday 07/31 at 6:30PM**

6. **REQUIRED TEXT**

None – Papers to be provided

7. UNIVERSITY STATEMENTS

CLASS REGISTRATION REQUIRED: Students not officially enrolled in a course offered by the university may not attend class according to university policy. Faculty are responsible for upholding this policy and may not add students to a class roster in Canvas.

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. Items submitted for this course may be submitted to TurnItIn.com for analysis.

STUDENT COPYRIGHT INFORMATION

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.

ACCOMMODATIONS AND ACCESSIBILITY CONCERNS

If you are seeking accommodations (class/course adjustments) for a disability, here are the steps to take:

1. Register as a student with a disability with Student Access Services (SAS) in the Center for Teaching and Learning (CTL). This process takes time, so engage with SAS as early as possible.
2. Once registered with SAS, you may be approved for accommodations by SAS. Approved accommodations will be listed on a "Faculty Contact Sheet" (FCS), and you will receive a copy of this FCS from SAS.
3. Meet with each of your instructors as soon as possible to review your accommodations as per the FCS and have them sign the FCS. This document will help you and your instructors develop a plan for providing the approved accommodations.
4. Let SAS know if you have any concerns about how your accommodations are being implemented in the classroom.

Please remember that:

1. The steps above are required in order to be granted reasonable accommodations for disabling conditions.
2. Accommodations cannot be implemented retroactively. That is, accommodations can only be applied to a course *after* they have been approved by SAS, and *after* you have discussed your accommodations with your instructor and the instructor has signed the FCS.
3. Appointments with SAS staff are scheduled through the Starfish "Success Network" tab (you can access Starfish through Canvas). For more information, check the SAS website, e-mail access@marymount.edu, or call 703-284-1538.

Temporary Challenges

Temporary challenges due to accident, illness, etc. that may result in missing class or navigating general campus access do not necessarily fall under the purview of SAS. If you experience something of this nature, please start by alerting your instructors. The Dean of Student Success may be involved in alerting instructors in extreme cases.

EMERGENCY NOTIFICATION POLICY

When students are absent due to a crisis situation or unexpected, serious illness and unable to contact their individual instructors directly, the Division of Student Affairs can send out an Emergency Notification. To initiate an Emergency Notification, students should contact the **Division of Student Affairs 703-284-1615** or student.affairs@marymount.edu. Emergency Notifications are **NOT** appropriate for non-emergency situations (e.g. car problems, planned absences, minor illnesses, or a past absence); are **NOT** a request or mandate to excuse an absence, which is at the sole discretion of the instructor; and are **NOT** a requirement for student absences. If a student contacts instructor about an emergency situation directly, it is not necessary to involve the Division of Student Affairs as arrangements are made to resolve the absence.

For non-emergency absences, students should inform their instructors directly.

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 confidentially.

UNIVERSITY POLICY ON WEATHER AND EMERGENCY CLOSINGS

Weather and Emergency closings are announced on Marymount's web site: **www.marymount.edu**, through **MUAlerts**, area radio stations, and TV stations. You may also call the **Weather and Emergency Hotline at (703) 526-6888** for 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 most timely 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., Canvas) for information on course work during periods in which the University is closed.