Katz
Katz School
of Science and Health

MS in Cybersecurity

Course Descriptions

CYB 5000 Cybersecurity Foundations

This course will prepare students for in-depth study and competency building in cybersecurity. Through hands-on work in understanding and applying cybersecurity frameworks and guidelines, students will explore general concepts, current standards and practices, and terminology. Students will be introduced to the most common cybersecurity functions, current and emerging cyber threats, challenges and solutions. The course will engage students in basic solutions design and applying techniques, using current case studies to introduce them to the operational factors, both non-technical and technical that address exposures and responses to cyber threats.

CYB 5100 Architecture of Secure Operating Systems, Applications, and Devices

As innovations involving sensing technology, robotics, and the Internet of Things are more frequently deployed in organizations, on vehicles, or around the home, businesses and personal safety can be highly dependent on the secure architecture of technology. Students will learn key concepts about technology access control design, fault and tamper resistance, testing, and common criteria used to determine if technology solutions are robust enough to withstand attacks such as tampering, denial of service, and unauthorized access.

CYB 5200 Network, Data, and Communications Security

Having a solid defense-in-depth strategy for architecting and operating networked technology provides organizations with operational resilience from cyber-attacks and data breaches. Students will learn key concepts about security architecture, network segmentation, defense-in-depth, encryption technologies, and backup/replication sites, including cloud-based servers and services.

CYB 5300 Risk Management and Cybersecurity

This course takes a multi-disciplinary approach to the study of risk governance and cybersecurity. Students will learn how to analyze, assess, control, and manage cybersecurity risks from the individual to the operational level. They will develop practical knowledge, analytical skills, and mathematical methods for calculating risk, as well as the artistic skills required to make decisions about which risks to control and how to control them.

CYB 5400 Cybersecurity Audit, Assessment and Training

This course will teach students how to assess and evaluate cyber security risks, conduct computer security audits, and test preparedness and response levels in the current technology environment. The course will explore standard evaluation and testing methodologies currently used across industries to identify and address cyber security threats. Students will also study current cyber policies used in both private and public sectors and their implementation.

TMG 5500 Leading Technology Organizations

Successful leaders require more than technical knowledge and skills: they must be able to identify and prioritize strategic challenges and opportunities and champion initiatives to address them. Students will master strategies for building short- and long-tern plans, developing a culture of productivity and

excellence, leading high performing teams, strengthening organizational communication, leading change management initiatives, and enabling the leadership potential of others. Additional topics may include individual and group behaviors, interpersonal relationships, and organizational structure and design. Importantly, students will learn the science behind strategic leadership in agile, high performing technology organizations.

ERM 5400 Business Continuity Planning and Crisis Communication

This course introduces students to the conceptual models, methods and tools of enterprise Business Continuity Management (BCM) and a key component, Global Crisis Communications Management. Students will be exposed to industry best practices and guidelines as developed by international BCM governance and organizations like the Business Continuity Institute (BCI) and the Disaster Recovery Institute (DRI) International. Students will explore how the BCM function provides an enterprise-wide, cross-border, and cross-functional vantage point and how organizations enhance organizational resilience through the strategic use of both the business continuity and cross-cultural crisis communications functions. Students will also review the many crisis communication management tools in use today, including emergency notification systems (ENS), as well as other international standards and crisis management plans.

ERM 6000 Emergency Management and Disaster Recovery

This course examines Organizational Emergency Management and Systems Disaster Recovery with an emphasis on the importance to an organization of having an emergency management and global IT disaster recovery plan. Major topics include planning for crises, developing levels of preparation, identifying factors that need to be managed, forecasting potential crisis situations, and examining key elements of an emergency management & IT disaster recovery plan.

ERM 6050 Cybersecurity and CyberTerrorism

This fundamentals course will introduce students to the principles of data and technology that frame and define cybersecurity. Students will gain insight into the importance of cybersecurity and the integral role of cybersecurity professionals. Students will explore foundational cybersecurity principles, security architecture, risk management, attacks, incidents, and emerging IT and IS technologies.

CYB 7992 E-Discovery, Digital Evidence & Computer Forensics

Electronic discovery has become a critical component of all major litigations as the key evidence increasingly consists of e-mail and electronic documents. This course will teach you the law of e-discovery, practical best practices provide exposure to the technology behind it all. The focus will be on making you competent as to the legal obligations of e-discovery.

MAN 5580 Project Management

This course teaches project management using several tools from the leading methodologies for managing software projects. The most effective project managers will combine methods to create a “right-sized” methodology appropriate to the organizational culture and project team members’ background and experience.

CYB 6300 Special Topics

This course provides the opportunity to offer boutique short-term courses on emerging phenomena, policies, processes, technologies, and techniques in cybersecurity. The expectation is that this will be an advanced class that requires an appropriate student project and deliverable in line with the number of credits awarded for the course.

CYB 6450 Independent Study

This independent study course provides the student with the flexibility to learn more about a topic of interest outside of the formal course setting. The subject should be chosen in consultation with a faculty

advisor who acts as the student's supervisor, and with the permission of the program director. The student is required to submit a course contract describing the course of study and its specific learning objectives. Course credit is determined in advance of the course, by the instructor with the approval of the program director.

CYB 6400 Internship

This course consists of an off-campus internship experience supervised by a staff person at the internship site and overseen by a faculty advisor. The internship site must be approved by the program director, and the overall duration of student work must be no less than 150 hours (based on a 3-credit course). At the start of the internship, the student and faculty advisor will jointly develop specific learning objectives tailored to the nature of the internship. Over the course of the internship, students will be required to submit weekly reflections, and at the end of the internship, students write a final paper that represents the culmination of the work performed.

CYB 6500 Capstone

In this course, students integrate the skills developed in previous classes into a comprehensive body of knowledge, and provide tangible evidence of these competencies. The Capstone has four components: 1) a brief proposal and project schedule; 2) the main project deliverable; 3) a final presentation; and 4) a reflection on the student’s cybersecurity management skills and competencies, with some depth in one or two areas of the profession and grounded in a particular real-world context.

Last Updated: 7/23//20