Katz
Katz School
of Science and Health

M.S. 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.

Industry Application: This course provides the foundational knowledge required for entry and advancement in cybersecurity roles and directly supports preparation for the CISSP (Certified Information Systems Security Professional) certification. Learners develop understanding of core security concepts, threat landscapes, governance principles, and how to integrate security into business operations across sectors such as financial services, healthcare, technology, and government. Emphasis on terminology, security functions, AI-augmented defense workflows, and real-world case studies aligns with the CISSP common body of knowledge and builds the analytical judgment needed to evaluate AI-enabled security tools, understand attacker motivations, and balance security controls with operational and business needs in complex organizational environments. Large language models (LLMs) and agentic AI are rapidly transforming cybersecurity operations, from threat intelligence analysis and automated incident triage to vulnerability assessment and compliance reporting, and are increasingly embedded in tools for log analysis, phishing detection, and security automation.

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.

Industry Application: As IoT, robotics, and embedded systems proliferate, secure architecture has become essential to organizational resilience and public safety. Industries such as automotive manufacturing, medical devices, and industrial automation face risks where cyber vulnerabilities can result in physical harm or operational disruption. Professionals must understand secure system design, access control, tamper resistance, and fault tolerance from the outset. This course prepares students to address the reality that security cannot be retrofitted; it must be architected into systems to withstand persistent and sophisticated attackers.

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.

Industry Application: Defense-in-depth network architectures are critical to preventing localized breaches from escalating into enterprise-wide incidents, increasingly augmented by AI security tools such as Darktrace for anomaly detection, CrowdStrike Falcon for endpoint threat hunting, SentinelOne for autonomous ransomware rollback, Lakera Guard for LLM prompt injection protection, and LLM Guard for data leakage prevention. Organizations require professionals who can implement AI-enhanced segmentation, encryption, layered controls, and runtime protections (e.g., Cortex XSIAM for incident triage, BurpGPT for predictive vulnerability scanning) to safeguard data across on-premises, cloud, and multi-tenant environments. Cloud providers and large enterprises also depend on resilient backup strategies and AI-driven compliance auditing (e.g., AccuKnox for policy generation). The course emphasizes that modern security balances prevention with AI-powered continuity, recovery, and threat intelligence—preparing professionals for environments where breaches are inevitable.

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.

Industry Application: Risk management frameworks provide organizations with structured, defensible approaches for making cybersecurity investment and governance decisions. This course prepares students to apply widely used risk and governance frameworks such as NIST Risk Management Framework (RMF), NIST Cybersecurity Framework (CSF), ISO/IEC 27005, and FAIR to identify, analyze, and prioritize cybersecurity risks. Organizations across regulated industries—including financial services, healthcare, and critical infrastructure—rely on these frameworks to meet regulatory expectations, guide enterprise risk decisions, and communicate risk consistently to executive leadership. By integrating quantitative risk analysis with qualitative judgment, students develop the ability to translate technical risks into business impact, enabling informed risk treatment decisions. This framework-based, business-aligned approach reflects

real-world practice and prepares graduates for roles in governance, risk, and compliance (GRC), security leadership, and CISSP-aligned risk management functions.

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.

Industry Application: Security audit and assessment capabilities are essential for validating controls, identifying gaps, and demonstrating compliance in increasingly cloud-centric environments augmented by AI tools. This course prepares students for cloud security assessment responsibilities aligned with the CCSK (Certificate of Cloud Security Knowledge), developing proficiency in evaluating cloud governance, shared responsibility models, data protection, identity and access management, and cloud risk controls using AI-enhanced methodologies. Key tools include Darktrace and CrowdStrike Falcon for anomaly detection and threat hunting; SentinelOne for automated vulnerability remediation; Lakera Guard and LLM Guard for LLM-specific audits (e.g., prompt injection and data leakage); AccuKnox for Kubernetes runtime compliance; and BurpGPT for predictive code scanning. Organizations across private and public sectors rely on these standardized, AI-powered audit methodologies to assess on-premises and cloud environments, meet regulatory obligations, and reduce exposure. The course equips students to perform systematic, evidence-based assessments using such tools, preparing them for roles in security auditing, GRC, and cloud security assurance where CCSK-aligned and AI-integrated knowledge is increasingly expected.

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.

Industry Application: Technology and cybersecurity professionals are frequently promoted into leadership roles without formal training in people management or strategy. Effective leaders must align technical initiatives with organizational goals, manage change, and foster productive team cultures. Security leaders, including CISOs, rely on these skills to build organizational buy-in, manage competing priorities, and drive long-term security maturity. The course emphasizes that leadership and communication skills are often the deciding factors between technical competence and career advancement.

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

ediscovery, 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.

Industry Application: Digital evidence and forensic analysis are central to modern incident response, litigation, and regulatory investigations, increasingly powered by LLM-driven tools for summarizing legal documents, extracting entities from unstructured evidence, and building agentic systems that autonomously triage alerts, correlate artifacts, and generate defensible investigative reports. This course supports CEH (Certified Ethical Hacker) knowledge areas by strengthening understanding of attack techniques, attacker behavior, and forensic artifacts, enhanced by AI security tools like Darktrace for anomaly detection, CrowdStrike Falcon for threat hunting, SentinelOne for ransomware rollback, Lakera Guard for prompt injection defense, and LLM Guard for data leakage prevention. Organizations, law firms, and incident response providers rely on professionals who can analyze compromised systems, preserve evidence, reconstruct attack timelines, and maintain legal defensibility using AI-augmented workflows. By integrating forensic analysis with adversarial perspectives and LLM-powered automation emphasized in CEH, the course prepares students for roles in digital forensics, incident response, and security investigations where ethical hacking and AI tool proficiency identify, validate, and document attacker activity.

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.

Industry Application: Security initiatives succeed or fail based on execution. Organizations value professionals who can manage scope, timelines, resources, and stakeholders while adapting project methodologies to organizational culture and complexity. Project management skills enable cybersecurity professionals to translate strategy into delivered outcomes, making them more effective contributors and positioning them for leadership roles.

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.

Industry Application: Cybersecurity evolves faster than static curricula can accommodate. Exposure to emerging threats, technologies, and techniques provides graduates with a competitive advantage and reinforces the importance of continuous learning. The project-based structure enables students to develop specialized expertise and portfolio artifacts that demonstrate adaptability and depth in rapidly changing security domains.

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.

Industry Application: Independent study cultivates self-directed learning and intellectual curiosity—traits highly valued in cybersecurity professionals. Employers seek individuals who can identify emerging problems, conduct independent research, and develop innovative solutions without prescriptive guidance. This course enables deep specialization and demonstrates initiative, distinguishing graduates in competitive hiring environments.

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.

Industry Application: Internships provide practical experience, professional networking, and exposure to real-world security operations. Employers frequently use internships as extended evaluations for full-time roles, making performance critical. Faculty oversight and structured learning objectives ensure meaningful engagement, skill development, and professional growth aligned with industry expectations.

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.

Industry Application: The capstone project provides tangible evidence of integrated cybersecurity competency. Employers value candidates who can scope problems, implement solutions, and communicate outcomes effectively. By grounding projects in real-world contexts, the capstone demonstrates readiness to contribute immediately in professional settings and supports portfolio-based evaluation by hiring managers.