University of San Diego | ONLINE

Is the Cybersecurity Pathway Right for You?

Through this Cybersecurity elective pathway, you'll receive an integrated introductory experience to cybersecurity developed in collaboration with industry, military, intelligence communities, and government stakeholders to deliver specific, in-demand knowledge and skill sets. The courses will provide essential knowledge and skills training for information security practitioners (public or private) who work to protect the safety and prosperity of companies, communities, and the nation. The goal is a real-world experience in which cybersecurity knowledge and skills can be applied in dynamic settings where innovation and problem-solving are required.

CYBR (Ex. CYBR 505 & CYBR 501) students will learn about digital and network forensics, the technical considerations for incident response and continuity planning, and much more. The program places students in simulated contestant cyber environments where they will perform system assessments, potentially on solutions they have engineered, and understand the various types of penetrations an adversary might attempt on an information system.

CSOL (Ex. CSOL 530 & CSOL 540) students will gain a deep understanding of cybersecurity concepts, topics and theories, along with leadership skills. In addition to cybersecurity leadership skills, students are taught theory and how to turn that theory into practice, gaining specific knowledge and skills in the areas of technology, law, policy, compliance, governance, intelligence, incident response, and management.

In preparation for your program start in the Cybersecurity pathway, please review the following program requirements:

Programming and Software Resources

- CompTIA Lab Simulation Service - CYBR 501 ($159)
  CompTIA is an online service for students working on certifications. It consists of courses taught through "lab sim (simulation)" with text, videos, labs, and assessments. Prepares students for: CompTIA Security Pro CompTIA Security+ (SY0-501).

CYBR Technical Resources and Requirements

- ***CYBR courses require students to have access to a Windows Operating System (OS)***
- ***OSX and Apple/Mac computers are not acceptable computers for the CYBR courses.***
- USD's Information Technology Services Hardware Recommendations
- Windows Operating System - 16 GB, 1.5 GHz Speed I7 + 500 GB external memory (preferably SSD hard disk drive). How-to-Check Guide Here!
- Speakers or headset – to listen and record multimedia.
- Webcam – for recording video.
- High-speed internet connection required.
- Browser Plug-ins – Windows Media Player, QuickTime, Adobe Reader, and Java.

- ➢ Microsoft Office is required (free with your USD account!)

CSOL Technical Resources and Requirements

- ➢ ***CSOL courses require a private computer, with full administrator privileges – a PC or Mac***
- ➢ USD's Information Technology Services Hardware Recommendations
- ➢ 16 GB and 1.5 GHz Speed I7 plus 500 GB external memory (preferably SSD hard disk drive) is recommended. How-to-Check Guide Here!
- ➢ Microsoft Office is required (free with your USD account!)
- ➢ Mozilla Firefox and Google Chrome are the recommended browsers. (You will want to have 2 browsers for software testing and viewing.)
- ➢ Speakers or headset – to listen and record multimedia.
- ➢ Webcam – for recording video.
- ➢ High-speed internet connection required (DSL or better).
- ➢ Browser Plug-ins – Windows Media Player, QuickTime, Adobe Reader, and Java.

Course Descriptions

The curriculum of this specialized track blends IT leadership core courses with cybersecurity-focused electives, as shown below.

ITL 535 Cybersecurity	This course will feature a comprehensive overview of concepts and tools essential to cybersecurity for IT professionals. Students will learn to view information as an asset to the organization, discover types of cybersecurity attacks, what threat actors are, the various roles of a cyber professional, and the beginnings of designing a cybersecurity program. Students will also identify different threats to information and the infrastructure and operators that support it. This course will also cover the risk management practices and principles that pertain to the cyber domain, as well as risk mitigation strategies, risk calculation, and communication and training for a cybersecurity program.
CYBR 505 Computational Roots of Cyber Security	This course is a prerequisite for the MS in Cyber Security Engineering program. Students without specific training in cyber engineering and/or an undergraduate degree in computer science, engineering or computer engineering may be required to take this course. Computational Roots of Cyber Security is an accelerated introduction to computer systems that provides essential education in the fundamentals. Three areas of computation are addressed in this course: Understanding how 1) programs work at a fundamental level (computer architecture), 2) how programs are managed and controlled (operating systems), and 3) how programs are constructed (programming) will be critical to the students' ability to comprehend the material of subsequent courses.
CYBR 501 Introduction to Cybersecurity Concepts and Tools	An introduction to the fundamentals of cybersecurity, including the notion of policy as the definition of "security" for a system and the concepts of threats, vulnerabilities, and risk. We will survey common attacks and mitigations, and the shortcomings of common, contemporary cybersecurity models. Students will practice aspects of networking, operating systems, and security test tools through computer virtualization and hands-on labs

	and will assemble a penetration testing Cybersecurity Sandbox with multiple virtual machines that they will use in subsequent courses and will demonstrate the use of a set of security test tools. Prerequisites: CYBR 505 (can be waived by MS-CSE Program Director based on student's academic and professional background)
CSOL 530 Governance and Risk in Cybersecurity	This course discusses and explains the fundamentals of risk governance, the processes to follow, compliance regulation, and the security controls to implement for specific cybersecurity environments and situations. Information and information systems are subject to serious threats that can have adverse impacts on organizational operations (including mission, functions, image, and reputation). Cyber-attacks are often aggressive, well-organized, well-funded, and in a growing number of documented cases, very sophisticated. There is also a geopolitical part to cybersecurity as well that is discussed throughout this course. Successful attacks on public and private sector information systems can affect organizational assets, individuals, other organizations, and the Nation by compromising the confidentiality, integrity, or availability of information being processed, stored, or transmitted by those systems. This can result in serious damage to the national and economic security interests of the United States.
CSOL 540 Cybersecurity Law and Policy	This course provides students with an introduction to and discusses the relationship between cybersecurity, cybersecurity law and privacy law, and “reasonable security measures”. The students will learn the responsibilities of a cybersecurity professional and cybersecurity counselor. The course will explore laws, regulations, and policies; enforcement, compliance, and litigation; consumer data privacy; US federal, state, and EU laws; and future trends.