CYBERSECURITY RISK MANAGEMENT PROGRAM

In this ten-week program, participants devise an operational cybersecurity risk management strategy using the NIST Cybersecurity Framework for a cyber-physical system or a technology of their choice.

DePaul University's Cybersecurity Risk Management Program provides the knowledge and skills essential for an effective response to advanced cybersecurity threats in any operational environment.

The program is ideally suited for information technology professionals and managers interested or involved in cybersecurity decision-making. The curriculum is flexible and meets the learning objectives of each participant. They can choose to apply the NIST Cybersecurity Framework to a technology they currently work with, are interested in, or use the Cyber-Physical Systems Lab at DePaul University [1].

The program addresses the benefits of a cybersecurity management strategy that includes consideration of ethical, legal, and privacy issues; an understanding of security standards and modern technology; an assessment of threats, vulnerabilities, and risks; and application of the principles of economics for cybersecurity. Classroom lectures and demonstrations will be complemented by readings, case study exercises, and a final project.

YOU WILL BE ABLE TO:

- design, implement, and sustain a strategy for operational cybersecurity risk management
- apply the NIST Cybersecurity Framework in any operational environment including cyber-physical systems (i.e., IoT and industrial process control systems)
- plan and conduct standardized cybersecurity threat and risk assessment for an operational environment
- experiment with tools and techniques for vulnerability assessment
- develop cybersecurity policies
- apply the principles of economics for cybersecurity
- consider the legal, ethical, and regulatory environment as it relates to operating in cyberspace
CYBERSECURITY RISK MANAGEMENT PROGRAM

CURRICULUM

INTRODUCTION Program overview. Program schedule and organization. The goals of comprehensive operational cybersecurity management strategy. Overview of the NIST Cybersecurity Framework.

THREAT ASSESSMENT Classification and identification of threat events, threat actors, and their characteristics. Estimating likelihood of initiating a cyberattack that results in adverse effects.

VULNERABILITY ASSESSMENT Classification and identification of vulnerabilities, severity, and predisposing conditions. Estimation of the likelihood that an initiated cyberattack will succeed.

RISK ASSESSMENT Estimation of level of impact of a cyberattack. Qualitative and quantitative risk assessment. The elements of the NIST Cybersecurity Framework.

CORE CYBERSECURITY RISK MANAGEMENT Identification of the core cybersecurity risk management activities per NIST Cybersecurity Framework categories, subcategories, and informational references.

LEGAL ISSUES, REGULATION, ETHICS State, federal, and international laws involving cyberattacks, breaches, and information misuse. Codes of conduct. Professional organizations. Cultural differences.

SECURITY TRAINING AND AWARENESS Organizational security culture. Cybersecurity trainings. Strategies for raising cybersecurity awareness.


ECONOMICS OF CYBERSECURITY Return of cybersecurity investment. Cybersecurity insurance.

OPERATIONAL RISK MANAGEMENT STRATEGY Application of the NIST Cybersecurity Framework in operational environment. Devising implementation, maintenance, and security maturation plans.
GENERAL INFORMATION

ADMISSION

Professional work experience in the administration, support, management, or risk assessment of security services is recommended. Applicants are expected to have knowledge of information and communication technologies and basic security knowledge.

A substantial commitment of time is required for this intensive course of study. Final admission will be determined by the admissions committee on the basis of an applicant's overall qualifications, including work history and educational background.

LAB EXPERIMENTATION

Participants interested in working with cyber-physical systems equipment can use DePaul CDM’s Cyber-Physical Systems Lab or bring IoT devices of their own (if preferred).

SCHEDULE

The Institute offers one section of the program each quarter. Classes meet once a week at a specially-equipped classroom in DePaul’s Loop Campus.

FACULTY

The program is taught by Filipo Sharevski, PhD, Director of DePaul’s Information Assurance Center and an expert in applied cybersecurity. He is responsible for both Secure Design Lab (SDL) and the Cyber-Physical Systems Lab (CPSL) at DePaul University where he leads research in the domain of secure design for IoT, industrial process control security, as well as critical infrastructure security.

REFERENCES

COLLEGE OF COMPUTING AND DIGITAL MEDIA

The college, through its School of Cinematic Arts, School of Computing, and its School of Design, offers a variety of programs at the undergraduate and graduate levels. Over 3,000 students are enrolled in the college’s bachelor’s programs and about 2,000 students are enrolled in the master’s and Ph.D. programs making the college’s graduate program one of the largest in the country. The college offers close to 400 courses each quarter, many in the evening, and primarily in the Loop and Lincoln Park Campuses. Most of the degree programs are also available exclusively online.

Offerings at the undergraduate level include:
- Animation B.A. / B.F.A.
- Computer Science B.S.
- Cyber-Physical Systems Engineering B.S.
- Cybersecurity B.S.
- Data Science B.S.
- Film and Television B.A. / B.F.A.
- Game Design B.S.
- Game Programming B.S.
- Graphic Design B.F.A.
- Information Systems B.S.
- Information Technology B.S.
- Interactive and Social Media B.S.
- Information Systems B.S.
- Information Technology B.S.
- Network Engineering and Security B.S.
- User Experience Design B.S.

Offerings at the graduate level include:
- Animation M.A.
- Applied Technology M.S.
- Computational Finance M.S.
- Computer Science M.S.
- Cybersecurity M.S.
- Data Science M.S.
- Digital Communication and Media Arts M.A.
- E-Commerce Technology M.S.
- Experience Design M.A.
- Film and Television M.S.
- Game Programming M.S.
- Health Informatics M.S.
- Human-Computer Interaction M.S.
- Information Systems M.S.
- Network Engineering and Security M.S.
- Product Innovation and Computing M.S.
- Software Engineering M.S.
- J.D./M.S. in Computer Science Technology

Master’s of Fine Arts
- Animation
- Creative Producing
- Documentary
- Film and Television Directing
- Game Design
- Screenwriting

Ph.D. in Computer and Information Sciences
- Ph.D. in Human Centered Design

INSTITUTE FOR PROFESSIONAL DEVELOPMENT

The Institute for Professional Development was formed by the college in 1984 to assist both individuals and businesses in keeping pace with the rapid development of computer technologies. The Institute currently offers a variety of intensive certificate programs in these areas:

- Advanced SQL
- Big Data and NoSQL
- Big Data Using Hadoop
- Big Data Using Spark
- Cloud Computing Technologies
- Cybersecurity Risk Management
- Data Science for Business
- Fundamentals of R
- Fundamentals of Software Testing
- Incident Response and Digital Forensics
- Introduction to SQL
- iOS Developer
- IPv6
- Java™ Developer
- Modern Information Technology
- Modern .NET Web Development
- SQL Server® Business Intelligence
- SQL Server® Database Administration
- Technology and Innovation
- Web Development with JavaScript and HTML5

APPLICATION PROCEDURE:

Complete the enclosed application and return it with a non-refundable $40.00 application fee (check or money order made payable to DEPAUL UNIVERSITY) to:

DePaul University
Institute for Professional Development
243 S. Wabash Avenue, Room 301
Chicago, IL 60604-2300

The Cybersecurity Risk Management Program at DePaul University is an independent program of study and is not affiliated with, nor has it been authorized, sponsored, or otherwise approved by external entities.