M.A. CYBERSECURITY / JURIS DOCTOR (J.D.) DUAL DEGREE

Students in the RWU School of Law are able to participate in a special dual degree opportunity with the M.A. in Cybersecurity program. The dual degree is designed to give students the foundational understanding of cybersecurity as it applies to the judicial process and provides students with the skills to effectively prosecute cybersecurity cases, analyze electronic evidence in court proceedings, engage information security analysts in legal casework, and more.

Dual degree students benefit from 12 credits of shared coursework that is transferable from each respective program to the other, providing a substantial cost and time savings over completing the degrees separately. ABA regulations require that students pursue one year of coursework in the School of Law prior to completing any master's coursework as a dual degree student.

Required Courses
(18 Credits in Cybersecurity)

SEC 502 Cybersecurity Fundamentals

SEC 550 Computer Networks

SEC 520 Digital Forensics

SEC 530 Principles of Cyber Intelligence

SEC 605 Cybersecurity & Networks Auditing

SEC 650 Advanced Problems in Cybersecurity

Plus 12 credits from the J.D. program in the RWU School of Law

ADMISSION REQUIREMENTS

Applications to the Cybersecurity programs are due by August 1 for fall admission, December 15th for spring admission, and April 15th for summer admission. To be considered for admission to the master's degree or graduate certificate programs, applicants must hold an earned bachelor's degree from an accredited college or university.

To apply, applicants must submit the following items to the Office of Graduate Admission:

1. Completed online application form and application fee

2. Official transcripts of all undergraduate and graduate coursework

3. Letter of intent (two double-spaced pages maximum) describing your interest in Cybersecurity, relevant past experiences and career goals

4. Master's candidates only: Two letters of recommendation attesting to your potential to succeed in graduate school

5. If your first language is not English, an official report of TOEFL or IELTS results

To read more about the application process and how to submit your materials, please visit **grad.rwu.edu/apply.**

Note: The GRE is not required for admission

EMPLOYERS OF OUR GRADUATES

> Blue Cross & Blue Shield of Rhode Island
> Brown University
> Fidelity Investments
> FLEXcon
> Innovative Defense Technologies (IDT)
> Mandiant
> Raytheon Technologies
> Rhode Island Airport Corporation
> Secureworks
> Sinapi Law Associates
> Sontiq
> Town of Portsmouth, RI
> U.S. Department of Homeland Security

CYBERSECURITY

Serving one of today's most in-demand job fields, the graduate programs in Cybersecurity provide students both with and without a technical background the foundational and advanced expertise to apply cybersecurity principles in current roles or to pursue new careers in information security. Designed with busy working professionals in mind, all cybersecurity coursework is offered in an asynchronous online format, allowing students to complete coursework on their own schedule.

The graduate programs in Cybersecurity were developed collaboratively with a board of industry professionals, providing education that is deeply rooted in professional practice. Students can pursue a short course of study to earn one of three graduate certificates or complete one of the two master's degrees. Certificates can also be stacked with a thesis to automatically earn the Master of Science in Cybersecurity.

The M.A./M.S. Cybersecurity programs were named to *Fortune Magazine's* Best Online Master's in Cybersecurity Degrees in 2022.

CYBERSECURITY PROFESSIONALS ARE IN DEMAND

According to Cyberseek.org, there are more than 570,000 cybersecurity job openings as of Augus 2023. The Bureau of Labor Statistics also reports that cybersecurity job openings are expected to grow by 35 percent by 2031 compared to only 5 percent across all occupations.

Program Options
> M.A. Cybersecurity
> M.A./J.D. Cybersecurity Dual Degree
> M.S. Cybersecurity
> Cybersecurity Certificate
> Cyberspecialist Certificate
> Digital Forensics Certificate
> Cloud Computing Certificate

Course Delivery
Asynchronous online

Key Features
> Technical and non-technical program options
> Stackable certificates
> Fully online curriculum

MASTER OF ARTS IN CYBERSECURITY

The M.A. in Cybersecurity is designed for professionals without a technical background who wish to understand cybersecurity applications in their work. This curriculum is appropriate for those who wish to analyze cybersecurity threats to business and infrastructure and create strategies to mitigate risks.

Students in the program will understand the legal, managerial, and policy implications of cybersecurity work and conduct research prior to completin the program. Graduates will possess the adequate preparation to pursue N+ and S+ certifications and take the exam to become a Certified Information Systems Security Professional (CISSP).

Required Courses (30 credits)

SEC 502 Cybersecurity Fundamentals

SEC 550 Computer Networks

SEC 529 Cybersecurity Tools and Applications

SEC 517 Information Risk Management

SEC 520 Digital Forensics

SEC 521 Mobile Device Forensics

SEC 530 Principles of Cyber Intelligence

SEC 605 Cybersecurity & Networks Auditing

SEC 640 CISSP Certification

SEC 650 Advanced Problems in Cybersecurity

MASTER OF SCIENCE IN CYBERSECURITY

The M.S. in Cybersecurity is designed for technical professionals or those with prior education in computer science or information technology. Coursework is designed to prepare students for roles as information security analysts or similar careers and utilizes virtual environments to simulate the systems and activities students will encounter in real-world applications.

Students in the program will acquire skills in computer programming, networking, assessment and analysis, forensics, and reporting that combine technical knowledge, situational management, and problem solving. Those without demonstrated technical coursework or professional experience will complete a series of networking and programming prerequisites prior to entry in the program. The program is designed around industry certifications and standards and provides a diverse background leading to entry-level careers (for those transitioning from other areas) and career advancement (for those with prior background in technology).

Required Courses (30 credits)

SEC 502 Cybersecurity Fundamentals

SEC 550 Computer Networks

SEC 507 Advanced Python programming

SEC 515 Intrusion Detection Systems

SEC 516 Cloud Architecture

SEC 525 Advanced Cryptography & Network Security

SEC 531 Penetration Testing

SEC 520 Digital Forensics

SEC 640 CISSP Certification

SEC 650 Advanced Problems in Cybersecurity

CYBERSECURITY GRADUATE CERTIFICATE

This certificate allows individuals the opportunity to explore the foundations of cybersecurity without a technical background. Courses in the certificate explore conceptual ideas related to cybersecurity networking and protection, auditing for compliance with state and federal regulations, and U.S. cybersecurity strategy and the macro-level impacts of individual network and system security.

Required Courses (9 credits)

SEC 502 Cybersecurity Fundamentals

SEC 530 Principles of Cyber Intelligence

SEC 605 Cybersecurity & Networks Auditing

CYBERSPECIALIST GRADUATE CERTIFICATE

This certificate allows individuals with a technical background to expand their cybersecurity skillset with advanced coursework in firewalls and security defense, cyberattack assessment, malicious code and malware analysis and prevention, and penetration testing

Required Courses (9 credits)

SEC 515 Intrusion Detection Systems

SEC 522 Malware Analysis

SEC 531 Penetration Testing

DIGITAL FORENSICS GRADUATE CERTIFICATE

The study of digital forensics is a growing field for both law enforcement as well as corporate employees. Within this five-course certificate, students will learn the techniques in common practice for the examination of digital media, forensic data recovery, data preservation, and presentation of technical evidence in court. Students will also explore the context of digital forensics under U.S. and International law.

Required Courses (9 credits)

SEC 520 Digital Forensics

SEC 501 Forensic Hardware and Acquisition

SEC 521 Mobile Device Forensics

CLOUD COMPUTING CERTIFICATE

The demand for cloud computing professionals has never been higher. Cloud skills are in high demand as companies strive to derive the most value from cloud-based technology. Global job site, Indeed.com concurs, identifying cloud skills as a major trend in the tech skills market. Applicants must hold a bachelor's degree from a regionally accredited college or university to be eligible for Graduate Certificate Admission.

Required Courses (9 credits)

SEC 516 Cloud Architecture

SEC 527 Clouds and Web Services Security

SEC 550 Computer Networks

"The program is designed around industry certs and standards and shall provide a diverse background leading to entry-level careers (for those transitioning from other areas) and career advancement (for those with prior background in technology)."

– Shakour Abuzneid,
  Professor of Cybersecurity and Networks