CYBERSECURITY (MS)

Program Director: Justin Del Vecchio, PhD (delveccj@canisius.edu)

The master of science in cybersecurity is designed to train professionals to protect the electronic data of businesses, educational institutions, government agencies and beyond. The program provides a cutting-edge curriculum that prepares graduates to succeed as a cybersecurity professional or researcher.

The cybersecurity MS is offered on campus with full- and part-time options. Students without a computer science background take a set of foundation courses to get them up to speed with the program. Students with a computer science background could have foundation courses waived at the discretion of the program director. The program aligns with curricular recommendations from the ACM Cybersecurity Curricula and the NSA's Center of Academic Excellence (CAE) in Cyber Defense.

Program courses are taught by industry professionals who are at the forefront of cybersecurity. Instructors guide students in hands-on lab exercises on topics including ethical hacking, securing development practices, analysis of malware samples and more. Students gain exposure to the most current tools and practices used in cybersecurity, including new courses for evolving topics.

Canisius Cybersecurity is also a proud member of the USCYBERCOM Academic Engagement Network. This affiliation provides insight into cutting edge cybersecurity issues used to develop course content.

Admissions Requirements

- Students from any undergraduate major are welcome to apply, as long as they have acquired a bachelor's degree prior to the start of classes.
- Cumulative GPA of 2.8 or higher.
- Students may apply at any time. We have rolling admissions.
- Student preparation and background are used to determine whether some foundation courses can be waived.

Materials to be Submitted

- Online Application (https://www.canisius.edu/admissions/apply-canisius/), with personal statement
- An official transcript from each college attended
- Resumé
- Two Letters of Recommendation
- Official GRE or GMAT score (optional)

Policies

Academic Standing

The cybersecurity program follows the College of Arts and Sciences on students' academic standing. (http://catalog.canisius.edu/graduate/academics/academic-policies/#academicstandingtext)

Matriculation and Continued Program Enrollment

The cybersecurity program follows the Canisius University policy for matriculated students (http://catalog.canisius.edu/graduate/admission-matriculation/#Matriculation) that expects students to maintain a continuous program of academic work.

Registration and Credit Hours

Cybersecurity students must be registered for at least 4.5 credits per semester to maintain eligibility for financial aid (if they are eligible). A full load is at least 9 credit hours. No student may register for more than 12 credit hours in any semester.

Curriculum

Foundation Course Help Make Your Program Yours

This program features foundation courses that are designed to work with your level of education and experience, so whether you're completely new to the field or a seasoned pro, this program is designed to work for you.

- **Foundation courses get you up to speed**. If you're a new college graduate or a career changer with little or no experience in the field, you can develop the skills and knowledge that you need for long-term success right at the beginning of your program.
- **Foundation courses can be waived with relevant experience at the discretion of the program director**. If you've mastered the basics and are looking to deepen your knowledge and hone your skills even further, you can get right into the material – and get to degree completion faster.

Code	Title	Credits
Foundation Courses (can be waived at the program director's discretion)		
CSC 511 & 511L	Introduction to Programming and Introduction to Programming Lab	3
CSC 512 & 512L	Data Structures and Algorithms and Data Structures and Algorithms Lab	3
Required Courses		
CSC 610 & 610L	Database Management and Database Management Lab	3
CYB 500 & 500L	Cybersecurity Principles and Cybersecurity Principles Lab	3
CYB 510	Cybersecurity Policies, Ethics, and Law	3
CYB 520 & 520L	Ethical Hacking and Penetration Testing and Ethical Hacking and Penetration Testing Lab	3
CYB 540 & 540L	Network and Internet Security and Network and Internet Security Lab	3
CYB 600 & 600L	Secure Software Engineering and Secure Software Engineering Lab	3
CYB 610	Cybersecurity Project	3
Choose from the following (9 credit hours):		**9**
CYB 505	Capture the Flag & Cybersecurity	
CYB 506	Cybersecurity Certification Preparation	
CYB 550 & 550L	Techniques to Analyze and Evaluate Malware and Techniques to Analyze and Evaluate Malware Lab	
CYB 580	Cybersecurity Seminar	
CYB 599 & 599L	Cybersecurity Special Topics and Cybersecurity Special Topics Lab	
CYB 611	Cybersecurity Thesis	
CYB 620 & 620L	Applied Cryptography and Applied Cryptography Lab	
CYB 655 & 655L	Cybersecurity Operations and Cybersecurity Operations Lab	
CYB 680	Cybersecurity Research	
CYB 697	Cybersecurity Internship	

CYB 699	Advanced Cybersecurity Topics
DAT 511	Data Stewardship: Preparation, Exploration and Handling of Big Data
DAT 514 & MAT 500	Data Mining and Machine Learning and Topics in Applied Mathematics (The combination of these two courses fulfills the elective credits)
Total Credits	**36**

Courses

Computer Science (CSC) (p. 2), Cybersecurity (CYB) (p. 2), Data Analytics (DAT) (p.), Mathematics (MAT) (p.)

Computer Science (CSC)

CSC 511 Introduction to Programming **3 Credits**
This foundational course will teach you the basics of computer programming using the Python language. You will design, code, test, and debug computer programs for textual and graphical applications.
Corequisite: CSC 511L.
Offered: every fall & spring.

CSC 511L Introduction to Programming Lab **0 Credits**
Required lab for CSC 511.
Corequisite: CSC 511.
Offered: every fall & spring.

CSC 512 Data Structures and Algorithms **3 Credits**
Introduction to object-oriented programming, recursion, and data structures, including lists, stacks, queues, trees and maps. Rudimentary discussion of analysis of algorithms. Python language used.
Prerequisite: CSC 511 or CSC 111. **Corequisite:** CSC 512L.
Offered: every fall & spring.

CSC 512L Data Structures and Algorithms Lab **0 Credits**
Required lab for CSC 512.
Corequisite: CSC 512.
Offered: every fall & spring.

CSC 530 Operating System Design **3 Credits**
The design of operating system software, including classic OS topics (scheduling, memory management, resource allocation and security) along with newer concepts including cloud computing and virtual machines. Taking CSC 253+lab or equivalent hardware course before this course is highly advised.
Prerequisite: A minimum grade of C in CSC 512 & CSC 512L.
Offered: every fall.

CSC 610 Database Management **3 Credits**
Databases, SQL language, concepts of normalization and database design. Rudimentary discussion of data ethics and security. MySQL or SQLite used.
Prerequisite: CSC 112 or CSC 512; may be taken concurrently.
Offered: every fall.

CSC 610L Database Management Lab **0 Credits**
Required lab for CSC 610.
Prerequisite: CSC 512L. **Corequisite:** CSC 610.
Offered: every fall.

Cybersecurity (CYB)

CYB 500 Cybersecurity Principles **3 Credits**
This course examines the landscape and the broad areas of cybersecurity which includes topics such as: Symmetric & Public-Key Encryption, Access Control, Database Security, Malware, DoS (Denial-of-Service) Attacks, Intrusion Detection & Firewalls, Software Security, Security Management & Policies, Internet Security, and Legal & Ethical Aspects of Cybercrime. Students will also complete hands-on labs and exercises to reinforce their working knowledge of computer, network and information security topics.
Prerequisite: (CSC 310 and CSC 310L) or (CSC 610 and CSC 610L) may be taken concurrently, and (CSC 112 and CSC 112L) or (CSC 512 and CSC 512L).
Corequisite: CYB 500L.
Offered: every fall & spring.

CYB 500L Cybersecurity Principles Lab **0 Credits**
Required lab for CYB 500.
Corequisite: CYB 500.
Offered: every fall & spring.

CYB 501 Cybersecurity Principles for Business **3 Credits**
This course examines the landscape and the broad areas of cybersecurity which includes topics such as: Symmetric & Public-Key Encryption, Access Control, Database Security, Malware, DoS (Denial-of-Service) Attacks, Intrusion Detection & Firewalls, Software Security, Security Management & Policies, Internet Security, and Legal & Ethical Aspects of Cybercrime.
Offered: every fall & spring.

CYB 505 Capture the Flag & Cybersecurity **1.5 Credits**
CTF stands for Capture The Flag. It's a competition where contestants solve challenges related to cybersecurity. These challenges can range from basic programming exercises to more complex tasks like hacking into servers to retrieve hidden data. The ultimate goal is to find a specific piece of text called the flag. Students will participate in weekly meetings and at least two CTF events in the semester.
Offered: every fall & spring.

CYB 506 Cybersecurity Certification Preparation **1.5 Credits**
This course is designed to prepare students for industry-recognized cybersecurity certifications, such as CompTIA Security+ or Certified Ethical Hacker (CEH). Participants will collaborate with the instructor to develop a personalized study plan, covering essential exam topics. Weekly meetings will focus on reviewing study materials, discussing best practices, and reinforcing key concepts. At the end of the course, students will take the target certification exam to validate their knowledge and skills.
Prerequisite: CYB 500.
Offered: every fall, spring, & summer.

CYB 510 Cybersecurity Policies, Ethics, and Law **3 Credits**
This course focuses on the managerial aspects of information security and assurance. Topics covered include access control models, information security governance, and information security program assessment and metrics. Coverage on the foundational and technical components of information security is included to reinforce key concepts. The course includes up-to-date information on changes in the field, such as national and international laws and international standards like the ISO 27000 series.
Offered: spring and summer.

CYB 520 Ethical Hacking and Penetration Testing **3 Credits**
This course provides an in-depth understanding of how to effectively protect computer networks. Students will learn the tools and penetration testing methodologies used by ethical hackers. In addition, the course provides a thorough discussion of what and who an ethical hacker is and how important they are in protecting corporate and government data from cyber attacks. Students will learn updated computer security resources that describe new vulnerabilities and innovative methods to protect networks. Also covered is a thorough update of federal and state computer crime laws, as well as changes in penalties for illegal computer hacking.
Prerequisite: CYB 500 and CYB 500L; may be taken concurrently.
Corequisite: CYB 520L.
Offered: every spring.

CYB 520L Ethical Hacking and Penetration Testing Lab **0 Credits**
Required Lab for CYB 520
Prerequisite: CYB 500 and CYB 500L.
Offered: every spring.

CYB 540 Network and Internet Security **3 Credits**
The purpose of this course is to provide a practical survey of network security applications and standards. The emphasis is on applications that are widely used on the Internet and for corporate networks, and on standards (especially Internet standards) that have been widely deployed. The first part of the course will cover a concise survey of the cryptographic algorithms and protocols underlying network security applications, including encryption, hash functions, message authentication, and digital signatures. The second part of the course will cover important network security tools and applications, including key distribution, Kerberos, X.509v3 certificates, Extensible Authentication Protocol, S/MIME, IP Security, SSL/TLS, IEEE 802.11i WiFi security, and cloud security. Finally, we will look at system-level security issues, including the threat of and countermeasures for malicious software and intruders, and the use of firewalls.
Prerequisites: CYB 500 (can be taken concurrently), and ((CSC 310 and CSC 310L) or (CSC 610 and CSC 610L)). **Corequisite:** CYB 540L.
Offered: every fall.

CYB 540L Network and Internet Security Lab **0 Credits**
Required lab for CYB 540
Corequisite: CYB 540.
Offered: every fall.

CYB 550 Techniques to Analyze and Evaluate Malware **3 Credits**
This course teaches a wide range of skills required to do malware analysis. Students will understand how cybersecurity analysts who evaluate malware perform their job and will learn the same skills they apply on a daily basis. The lecture component of the course will explain malware analysis concepts while the lab components will have students apply the concepts learned on actual malware. Specific topic coverage includes: Introduction to Malware Analysis, Basic Static Analysis Techniques, Advanced Static Analysis Techniques, Basic Dynamic Analysis Techniques, Advanced Dynamic Analysis Techniques, Basics of Assembly Language and Disassembly, Debugging, Disassembly with IDA and Ghidra, Packers and Cryptors, Android Malware, Malware Obfuscation Techniques, and Risk Mitigation .
Prerequisite: CYB 500 (can be taken simultaneously). **Corequisite:** CYB 550L.
Offered: every fall.

CYB 550L Techniques to Analyze and Evaluate Malware Lab **0 Credits**
Required lab for CYB 550.
Corequisite: CYB 550.
Offered: every fall.

CYB 580 Cybersecurity Seminar **3 Credits**
This a graduate seminar course in which students will give oral presentations of scientific data. Students attend presentations as well as prepare and present on various topics in cybersecurity for faculty and other students. The seminars is expected to enhance the student's public speaking skills and to provide experience in preparing scientific presentations for professional settings. To help students improve as speakers, each student will receive feedback from fellow students and the instructor.
Offered: occasionally.

CYB 599 Cybersecurity Special Topics **3 Credits**
Current topics in Cybersecurity of interested to faculty and students. Possible topics include: Malware Analysis & Reverse Engineering, Bitcoin & Cryptocurrencies, Machine Learning & Security, Computer Forensics, etc.
Prerequisites: CYB 500 can be taken concurrently. **Corequisite:** CYB 599L.
Offered: every fall.

CYB 599L Cybersecurity Special Topics Lab **0 Credits**
Required lab for CYB 599
Corequisite: CYB 599.
Offered: every fall.

CYB 600 Secure Software Engineering **3 Credits**
The purpose of this course is to provide secure programming practices that are necessary to develop applications that withstand cyber-attacks and common software exploits. The first part of the course will cover the fundamentals of software security and implementing a continuous risk management framework throughout the software development lifecycle. The second part of the course will cover the Seven Touchpoints for software security as well as code reviews and software penetration testing. Finally, we will look at adopting a secure development lifecycle (SDL) in an enterprise setting.
Prerequisite: CYB 500 and CSC 610. **Corequisite:** CYB 600L.
Offered: every spring.

CYB 600L Secure Software Engineering Lab **0 Credits**
Required lab for CYB 600
Corequisite: CYB 600.
Offered: every spring.

CYB 610 Cybersecurity Project **3 Credits**
This course requires the culmination of knowledge and laboratory experience gained from the MS in Cybersecurity program as students will have the opportunity to design and implement a graduate capstone project. Students may complete this project for a real-world application or in a laboratory-setting that pertains to the greater field of cybersecurity. Students must defend their work in an open project defense and complete a written report of their work before a letter grade is awarded.
Prerequisite: CYB 520.
Offered: every fall, spring, & summer.

CYB 611 Cybersecurity Thesis **3 Credits**
The purpose of the thesis course is to provide students the opportunity to work with a faculty advisor on a research problem in cybersecurity. Completion of the thesis will require scholarly research methods to produce a significant thesis document that is comparable to a peer-reviewed publication. This course should be taken during the last semester of the MS program and the final thesis and oral presentation (defense) will be evaluated by a faculty committee before a grade is awarded.
Prerequisite: CYB 610.
Offered: every fall & spring.

CYB 620 Applied Cryptography **3 Credits**
This course will introduce the concepts of modern cryptography, including a combination of both theoretical foundations and practical applications of cryptography used in the real world. This course complements all of the CYB 5xx cybersecurity courses by taking a deeper look into cryptography to grasp a better understanding of cryptographic primitives, algorithms, attacks, and protocols. At the end of this course, students will have a proper foundation of modern cryptography and be able to apply cryptographic techniques in the design and analysis of secure computing systems.
Prerequisites: CYB 520 and CYB 540 (CYB 540 can be taken concurrently).
Corequisite: CYB 620L.
Offered: every fall.

CYB 620L Applied Cryptography Lab **0 Credits**
Required lab for CYB 620
Corequisite: CYB 620.
Offered: every fall.

CYB 655 Cybersecurity Operations **3 Credits**
Defending an enterprise network from attackers and adversaries gets more complicated every year - this course aims to give students a taste of the different technologies and disciplines that are needed to detect and investigate potential intrusions. Topics covered include building and tuning logging infrastructure, detection engineering, honeypot deployments, threat intelligence, purple teaming, and incident response. The course is designed with an emphasis on hands-on, practical skills that are in common use in the cybersecurity industry today.
Prerequisite: CYB 540 and CSC 530. **Corequisite:** CYB 655L.
Offered: every fall.

CYB 655L Cybersecurity Operations Lab **0 Credits**
Defending an enterprise network from attackers and adversaries gets more complicated every year - this course aims to give students a taste of the different technologies and disciplines that are needed to detect and investigate potential intrusions. Topics covered include building and tuning logging infrastructure, detection engineering, honeypot deployments, threat intelligence, purple teaming, and incident response. The course is designed with an emphasis on hands-on, practical skills that are in common use in the cybersecurity industry today.
Prerequisite: CYB 540 and CSC 530. **Corequisite:** CYB 655.
Offered: every fall.

CYB 680 Cybersecurity Research **3 Credits**
A research experience in Cybersecurity conducted with and under the supervision of a faculty advisor.
Prerequisite: CYB 500/L and program director approval.
Offered: as needed.

CYB 697 Cybersecurity Internship **3 Credits**
The application of the knowledge and skills acquired from the MS in Cybersecurity program in a real-world professional setting. Students will be responsible for arranging a practicum/internship with a business or organization that is related to cybersecurity. The outline of work duties and evaluative methods are established by the student and the internship mentor/supervisor and approved by the faculty advisor prior to initiation of the course.
Prerequisite: CYB 500.
Offered: every fall, spring, & summer.

CYB 699 Advanced Cybersecurity Topics **3 Credits**
In depth study of a topic related to cybersecurity.
Prerequisite: permission of instructor.
Offered: occasionally.

Roadmap

Full-Time with CSC background

First Year

Fall	Spring	Summer
CYB 500 & 500L	CYB 520 & 520L	CYB 610
CYB 540L	CYB 620L	CYB 510
CYB 550	CYB 600 & 600L	

Second Year

Fall
CYB 620 & 620L
CYB 655
One (or comb0 or) of the following:
CYB 505
CYB 506
CYB 599 & 599L
CYB 611
CYB 697

Part-Time with CSC background

First Year

Fall	Spring	Summer
CYB 500 & 500L	CYB 520 & 520L	CYB 510
CYB 550	CYB 505	
	CYB 506	

Second Year

Fall	Spring
CYB 540 & 540L	CYB 600 & 600L
CYB 655	CYB 620

Third Year

Fall
CYB 610
And one of the following:
CYB 599 & 599L
CYB 611
CYB 697

Full-Time with no CSC background

First Year

Fall	Spring	Summer
CSC 511 & 511L	CSC 512 & 512L	CYB 697 (or CYB elective)
CYB 500	CSC 610 & 610L	
	CYB 500L	
	CYB 510	

Second Year

Fall	Spring
CSC 530	CYB 520 & 520L
CYB 540 & 540L	CYB 600 & 600L
CYB 550 & 550L	CYB 610

Part-Time with no CSC background

First Year		
Fall	**Spring**	**Summer**
CSC 511 & 511L	CSC 512 & 512L	CYB 510
CYB 500	CSC 610 & 610L	
Second Year		
Fall	**Spring**	**Summer**
CSC 530	CYB 520 & 520L	CYB 610
CYB 540 & 540L	CYB 600 & 600L	
Third Year		
Fall		
CYB 550 & 550L		
CYB elective		

Learning Goals and Objectives

On completing the MS program, students will be able to:

1. Assess risks and threats
   - Perform information security risk assessment, identify potential threats, and develop threat mitigation strategies.
   - Identify malicious activities and attacks, and recommend appropriate response capabilities.
   - Perform malware analysis to understand its construction and functionality.
2. Implement policies and respond to incidents
   - Describe security design principles and identify security mechanisms to implement desired security principles.
   - Implement security defense technologies.
   - Carry out incident response activities and support cyber-crime investigation.
   - Perform audit procedures, evaluate the strengths and weaknesses of the security mechanisms, and develop contingency plans.
3. Communicate and educate on cybersecurity Issues
   - Describe individual privacy rights, related laws and regulations, and the use of information assurance technologies to support the enforcement of these rights.
   - Describe the responsibilities of all levels of users related to the threats against information systems.
   - Communicate information security concepts to individuals with diverse levels of computing skills.