**CYBERSECURITY (MS)**

**Program Director:** Jeffrey Spaulding, PhD (/spauldjd@canisius.edu)

The M.S. in Cybersecurity program is designed to train cybersecurity professionals to meet the needs of business, industry, educational institutions, and government agencies locally and nation-wide. The program provides a cutting-edge curriculum that prepares graduates to succeed as a cybersecurity professional or researcher.

The Cybersecurity MS is designed as a full-time (with a part-time option), face-to-face program. Students without a computer science background may take a set of courses as preparatory that would otherwise be waived for those with the applicable undergraduate courses. The program is in line with curricular recommendations from the ACM Cybersecurity Curricula and the NSA’s Center of Academic Excellence (CAE) in Cyber Defense.

**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 if some introductory courses may be waived.

**Materials to be Submitted**

- Free Online Application (https://www.canisius.edu/admissions/apply-canisius/), with essay
- An official transcript from each college attended
- Official GRE or GMAT score (optional)
- Resumé (optional)
- One or two Letters of Recommendations (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 College 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**

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bridge Courses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSC 501 &amp; 501L</td>
<td>Introduction to Programming and Introduction to Programming Lab</td>
<td>3</td>
</tr>
<tr>
<td>CSC 502 &amp; 502L</td>
<td>Data Structures and Algorithms and Data Structures and Algorithms Lab</td>
<td>3</td>
</tr>
<tr>
<td>MAT 591</td>
<td>Discrete Mathematics</td>
<td>3</td>
</tr>
</tbody>
</table>

**Required Courses**

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSC 530 &amp; 530L</td>
<td>Operating System Design and Distributed Computing and Operating System Design and Distributed Computing Laboratory</td>
<td>3</td>
</tr>
<tr>
<td>CYB 500 &amp; 500L</td>
<td>Cybersecurity Principles and Cybersecurity Principles Lab</td>
<td>3</td>
</tr>
<tr>
<td>CYB 510</td>
<td>Cybersecurity Policies, Ethics, and Law</td>
<td>3</td>
</tr>
<tr>
<td>CYB 520 &amp; 520L</td>
<td>Ethical Hacking and Penetration Testing and Ethical Hacking and Penetration Testing Lab</td>
<td>3</td>
</tr>
<tr>
<td>CYB 540 &amp; 540L</td>
<td>Network and Internet Security and Network and Internet Security Lab</td>
<td>3</td>
</tr>
<tr>
<td>CYB 600 &amp; 600L</td>
<td>Secure Software Engineering and Secure Software Engineering Lab</td>
<td>3</td>
</tr>
<tr>
<td>CYB 610</td>
<td>Cybersecurity Project</td>
<td>3</td>
</tr>
<tr>
<td>CYB 620 &amp; 620L</td>
<td>Applied Cryptography and Applied Cryptography Lab</td>
<td>3</td>
</tr>
<tr>
<td>DAT 513 &amp; 513L</td>
<td>Database Management and Database Management Lab</td>
<td>3</td>
</tr>
<tr>
<td>CYB 599 &amp; 599L</td>
<td>Cybersecurity Special Topics and Cybersecurity Special Topics Lab</td>
<td>3</td>
</tr>
<tr>
<td>CYB 611</td>
<td>Cybersecurity Thesis</td>
<td>3</td>
</tr>
<tr>
<td>CYB 697</td>
<td>Cybersecurity Internship</td>
<td>3</td>
</tr>
</tbody>
</table>

**Total Credits:** 39

**Courses**

Computer Science (CSC) (p. 1), Cybersecurity (CYB) (p. 2), Data Analytics (DAT) (p. 3), Mathematics (MAT) (p. 3)

**Computer Science (CSC)**

**CSC 501 Introduction to Programming**

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.

**Offered:** every fall, spring, & summer.

**CSC 501L Introduction to Programming Lab**

Required lab for CSC 501.

**Corequisite:** CSC 501.

**CSC 502 Data Structures and Algorithms**

The primary focus of this course is data structures and their accompanying algorithms, including recursive algorithms. In order to judge between competing algorithms or alternative data structures, we will use analysis to discover the time and memory bounds of various approaches. We will also use object oriented programming as a useful way of constructing abstract data types and in general structuring complex programs. Several debugging tools and approaches will be explored, especially hand tracing of algorithms. The Python programming language will be our main vehicle.

**Prerequisite:** CSC 501 or CSC 111 as prerequisite. **Corequisite:** CSC 502L.

**Offered:** every fall, spring, & summer.
<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
<th>Credits</th>
<th>Offered</th>
<th>Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSC 502L</td>
<td>Data Structures and Algorithms Lab</td>
<td>0</td>
<td>Summer</td>
<td>Required lab for CSC 502.</td>
</tr>
<tr>
<td>CYB 500</td>
<td>Cybersecurity Principles</td>
<td>3</td>
<td>Every fall &amp; spring</td>
<td>A minimum grade of C in CSC 502 &amp; CSC 502L. Corequisite: CSC 500L.</td>
</tr>
<tr>
<td>CSC 500L</td>
<td>Operating System Design and Distributed Computing Laboratory</td>
<td>0</td>
<td>Every fall &amp; spring</td>
<td>Required lab for CSC 530. Corequisite: A minimum grade of C in CSC 502 &amp; CSC 502L. Corequisite: CSC 530L.</td>
</tr>
<tr>
<td>CYB 520</td>
<td>Ethical Hacking and Penetration Testing</td>
<td>3</td>
<td>Every spring</td>
<td>Prerequisite: CYB 500 and CYB 500L.</td>
</tr>
<tr>
<td>CYB 520L</td>
<td>Ethical Hacking and Penetration Testing Lab</td>
<td>0</td>
<td>Every spring</td>
<td>Required Lab for CYB 520.</td>
</tr>
<tr>
<td>CYB 540</td>
<td>Network and Internet Security</td>
<td>3</td>
<td>Every fall</td>
<td>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, SMTP, 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. Prerequisite: CSC 502, CYB 500, and DAT 513. Corequisite: CYB 540L.</td>
</tr>
<tr>
<td>CYB 540L</td>
<td>Network and Internet Security Lab</td>
<td>0</td>
<td>Every fall</td>
<td>Required lab for CYB 540.</td>
</tr>
<tr>
<td>CYB 580</td>
<td>Cybersecurity Seminar</td>
<td>3</td>
<td>Every fall</td>
<td>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. Prerequisite: CSC 502, CYB 500, and DAT 513. Corequisite: CYB 599L.</td>
</tr>
<tr>
<td>CYB 599</td>
<td>Cybersecurity Special Topics</td>
<td>3</td>
<td>Every fall</td>
<td>Current topics in Cybersecurity of interested to faculty and students. Possible topics include: Malware Analysis &amp; Reverse Engineering, Bitcoin &amp; Cryptocurrencies, Machine Learning &amp; Security, Computer Forensics, etc. Prerequisite: CSC 502 and CYB 500. Corequisite: CYB 599L.</td>
</tr>
<tr>
<td>CYB 599L</td>
<td>Cybersecurity Special Topics Lab</td>
<td>0</td>
<td>Every fall</td>
<td>Required lab for CYB 599.</td>
</tr>
<tr>
<td>CYB 600</td>
<td>Secure Software Engineering</td>
<td>3</td>
<td>Every spring</td>
<td>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: CSC 502, CYB 500, and DAT 513. Corequisite: CYB 600L.</td>
</tr>
<tr>
<td>CYB 600L</td>
<td>Secure Software Engineering Lab</td>
<td>0</td>
<td>Every spring</td>
<td>Required lab for CYB 600.</td>
</tr>
<tr>
<td>DAT 513</td>
<td>Database Management Systems</td>
<td>3</td>
<td>Every spring</td>
<td>Possible topics include: Malware Analysis &amp; Reverse Engineering, Bitcoin &amp; Cryptocurrencies, Machine Learning &amp; Security, Computer Forensics, etc. Prerequisite: CSC 502 and CYB 500. Corequisite: CYB 599.</td>
</tr>
<tr>
<td>DAT 513L</td>
<td>Database Management Systems Laboratory</td>
<td>0</td>
<td>Every spring</td>
<td>Required lab for DAT 513.</td>
</tr>
<tr>
<td>CSC 502</td>
<td>Operating System Design and Distributed Computing</td>
<td>3</td>
<td>Every spring</td>
<td>The design of operating system software, distributed applications, client/server and other models, security issues, and parallel programming on a High Performance Computing Cluster. Prerequisite: CSC 530L.</td>
</tr>
<tr>
<td>CSC 502L</td>
<td>Operating System Design and Distributed Computing Laboratory</td>
<td>0</td>
<td>Every spring</td>
<td>Required lab for CSC 502.</td>
</tr>
<tr>
<td>CSC 502L</td>
<td>Operating System Design and Distributed Computing Laboratory</td>
<td>0</td>
<td>Every spring</td>
<td>Required lab for CSC 502.</td>
</tr>
<tr>
<td>CSC 530</td>
<td>Operating System Design and Distributed Computing</td>
<td>3</td>
<td>Every spring</td>
<td>The design of operating system software, distributed applications, client/server and other models, security issues, and parallel programming on a High Performance Computing Cluster. Prerequisite: A minimum grade of C in CSC 502 &amp; CSC 502L. Corequisite: CSC 530L.</td>
</tr>
<tr>
<td>CSC 530L</td>
<td>Operating System Design and Distributed Computing Laboratory</td>
<td>0</td>
<td>Every spring</td>
<td>Required lab for CSC 530. Corequisite: A minimum grade of C in CSC 502 &amp; CSC 502L. Corequisite: CSC 530L.</td>
</tr>
<tr>
<td>CSC 502</td>
<td>Operating System Design and Distributed Computing</td>
<td>3</td>
<td>Every spring</td>
<td>The design of operating system software, distributed applications, client/server and other models, security issues, and parallel programming on a High Performance Computing Cluster. Prerequisite: A minimum grade of C in CSC 502 &amp; CSC 502L. Corequisite: CSC 530L.</td>
</tr>
<tr>
<td>CSC 530L</td>
<td>Operating System Design and Distributed Computing Laboratory</td>
<td>0</td>
<td>Every spring</td>
<td>Required lab for CSC 530. Corequisite: A minimum grade of C in CSC 502 &amp; CSC 502L. Corequisite: CSC 530L.</td>
</tr>
<tr>
<td>CSC 502</td>
<td>Operating System Design and Distributed Computing</td>
<td>3</td>
<td>Every spring</td>
<td>The design of operating system software, distributed applications, client/server and other models, security issues, and parallel programming on a High Performance Computing Cluster. Prerequisite: A minimum grade of C in CSC 502 &amp; CSC 502L. Corequisite: CSC 530L.</td>
</tr>
<tr>
<td>CSC 530L</td>
<td>Operating System Design and Distributed Computing Laboratory</td>
<td>0</td>
<td>Every spring</td>
<td>Required lab for CSC 530. Corequisite: A minimum grade of C in CSC 502 &amp; CSC 502L. Corequisite: CSC 530L.</td>
</tr>
<tr>
<td>CSC 502</td>
<td>Operating System Design and Distributed Computing</td>
<td>3</td>
<td>Every spring</td>
<td>The design of operating system software, distributed applications, client/server and other models, security issues, and parallel programming on a High Performance Computing Cluster. Prerequisite: A minimum grade of C in CSC 502 &amp; CSC 502L. Corequisite: CSC 530L.</td>
</tr>
<tr>
<td>CSC 530L</td>
<td>Operating System Design and Distributed Computing Laboratory</td>
<td>0</td>
<td>Every spring</td>
<td>Required lab for CSC 530. Corequisite: A minimum grade of C in CSC 502 &amp; CSC 502L. Corequisite: CSC 530L.</td>
</tr>
</tbody>
</table>
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.

Data Analytics (DAT)

DAT 513 Database Management 3 Credits
This course presents an introduction to the design and use of database systems. Traditional databases will be the primary focus, centering on the relational model (SQL and related tools). There will be some discussion of large-scale information retrieval in the form of the NoSQL movement and data mining. Ethical, social and security issues will also be covered in an introductory fashion.
Prerequisites: CSC 501 and CSC 502, or equivalent. Corequisite: CSC 502.
Offered: every fall & spring.

DAT 513L Database Management Lab 0 Credits
Required lab for DAT 513.
Prerequisite: CSC 502L. Corequisite: DAT 513.
Offered: every fall.

Mathematics (MAT)

MAT 591 Discrete Mathematics 3 Credits
Fundamental topics with computer science applications. Sets and logic, propositional and predicate calculus, elements of combinatorics and counting, elementary discrete probability, functions and relations, and graphs.
Offered: every fall.

Roadmap

Full-Time

First Year
Fall
CYB 500 & 500L
CYB 510
DAT 513 & 513L
CYB 520 & 520L
CSC 530 & 530L
CYB 600 & 600L
Second Year
Fall
CYB 540 & 540L
CYB 620 & 620L
One of the following:
CYB 599 & 599L
CYB 611
CYB 697

Part-Time

First Year
Fall
CYB 500 & 500L
DAT 513 & 513L
CYB 520 & 520L
Second Year
Fall
CYB 540 & 540L
CSC 530 & 530L
CYB 610
Third Year
Fall
CYB 620
& 620L
One of the following:
CYB 599
& 599L
CYB 611
CYB 697

Learning Goals & 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.

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.