CYBERSECURITY ANALYTICS AND OPERATIONS

Graduate Program Head: Jeffrey Bardzell
Program Code: CYMPS
Campus(es): University Park (M.S.), World Campus (M.P.S.)
Degrees Conferred: Master of Science (M.S.), Master of Professional Studies (M.P.S.)
The Graduate Faculty View (https://secure.gradsch.psu.edu/gpms/?searchType=fac&prog=CYMPS)

The Master of Science in Cybersecurity Analytics and Operations program is designed to create a deep understanding of cybersecurity analytics and operations, by blending education relating to technology, incident response, strategic planning, and crisis management. The program also aims to prepare the next generation of cybersecurity analysts to better protect digital information from attack through cybersecurity strategies, including incident response, strategic planning, and crisis management. With a foundation in mathematics and computer programming, students will be prepared to recognize, analyze, defend against, and manage risks related to a wide range of threats to online information, data stores, and networks. The program will be delivered in a resident format that takes one to two years. The total credits of the program is 30. A one-year program starts in a Fall semester, and concludes at the end of the following Summer.

The Master of Professional Studies in Cybersecurity Analytics and Operations (MPSCY) is an innovative program that targets professionals and organizational leaders who seek a professional education and training program. The purpose of the professional master's program is to produce professionals and organizational leaders who not only can select and draw upon the necessary foundations within the cybersecurity analytics and operations technology areas, test the applicability of these foundations for addressing a given issue, and apply the resulting solutions, but also can be aware of the multitude of technological trends and environmental factors that organizations must address in the changing global economy. The M.P.S. equips students to: understand and analyze the profound information and technological changes sweeping the world; meet challenges by developing innovative solutions using the foundations of cybersecurity analytics and operations; and have a clear advantage in today's highly competitive and dynamic environment by continuously learning new trends, issues, and innovations.

Admission Requirements
Applicants apply for admission to the program via the Graduate School application for admission (http://gradschool.psu.edu/prospective-students/how-to-apply/). Requirements listed here are in addition to Graduate Council policies listed under GCAC-300 Admissions Policies (http://gradschool.psu.edu/graduate-education-policies/).

Master of Professional Studies (M.P.S.)
Applicants to the M.P.S. program are required to submit three letters of reference, and a one-three page personal statement of relevant experience and goals. Because the M.P.S. program is multidisciplinary in nature, students from many different disciplines may be accepted for entry into the program. A bachelor's degree in a related area (e.g., engineering and science), while not necessary for admission, is helpful in the successful completion of the degree. It is expected that students will have a basic level of competency in statistics, as well as computer and information technology. Related work experience can be used to demonstrate such competency. A student may be accepted into the program with provisional status (http://gradschool.psu.edu/graduate-education-policies/gcac/gcac-300/provisional-admission/) for no more than one year while work is completed to meet these expectations.

It is expected that the successful applicant will have an overall grade point average of 3.00 (on a 4.00 scale) or higher for his or her undergraduate study and/or graduate-level study. However, accomplishments demonstrated through work experience and recommendation letters from the applicant's academic adviser or employer will also play an important role in making the admission decision. The most qualified applicants will be accepted into the program until all spaces for new students are filled.

Master of Science (M.S.)
Applicants to the M.S. program are required to submit three letters of reference, a current resume (including present position and any publications), 1 to 3 page statement of goals related to pursuing an advanced degree and career in IST and provide a sample of the applicant's writing (e.g. technical paper, etc.).

Because cybersecurity analytics and operations career opportunities exist in many disciplines, students with a wide range of disciplinary backgrounds may be accepted into the program. A bachelor's degree in a related area (e.g., engineering and science), while not necessary for admission, is helpful in the successful completion of the degree. However, it is expected that students will have a basic level of competency in mathematics and programming.

Entrance Requirement regarding Mathematics: Applicants must complete a Calculus course equivalent to Penn State University's MATH 110 or MATH 140.

Entrance Requirement regarding Programming: Applicants must complete two introductory-level programming courses where both courses used the same language. If an applicant believes his/her work experience satisfies the background, he/she should include a recommendation letter from a technical colleague describing the applicant's coding contributions at work. In addition, students who meet all other academic requirements, but need to improve identified gaps in specific programming skills areas, will have access to educational bridge materials to help improve certain knowledge domains.

It is expected that the successful applicant will have an overall grade point average of 3.50 (on a 4.00 scale) or higher for his or her undergraduate study and/or graduate-level study. However, accomplishments demonstrated through work experience and recommendation letters from the applicant's academic adviser or employer will also play an important role in the admission decision as well. The most qualified applicants will be accepted into the program until all spaces for new students are filled.

Degrees Conferred:
Master of Science (M.S.)
Master of Professional Studies (M.P.S.)
Degree Requirements

Master of Professional Studies (M.P.S.)

Requirements listed here are in addition to Graduate Council policies listed under GCAC-700 Professional Degree Policies (http://gradschool.psu.edu/graduate-education-policies/).

The M.P.S. program requires a minimum of 33 credits at the 400, 500, or 800 level, with at least 6 credits at the 500 level. These 33 credits are distributed among the following requirements:

- Required Courses
- Electives
- Culminating Experience

Elective Courses
The elective courses for the M.P.S. will be selected from a list maintained by the program office.

Culminating Experience
The student may choose one of two culminating experiences for the degree: either the capstone project guided by the student's adviser and completed while enrolled in IST 594, or the capstone course IST 894.

Master of Science (M.S.)

Requirements listed here are in addition to Graduate Council policies listed under GCAC-600 Research Degree Policies. (http://gradschool.psu.edu/graduate-education-policies/)

The M.S. in Cybersecurity Analytics and Operations requires a minimum of 30 credits at the 400, 500, 600, or 800 level, with at least 18 credits in the 500 or 600 series combined; 27 of the 30 credits must be earned at Penn State (refer to GCAC-309 Transfer Credit (http://gradschool.psu.edu/graduate-education-policies/gcac/gcac-300/gcac-309-transfer-credit/)). Students will be able to complete the proposed Master's program in one calendar year (including summer) or two academic years. All of the courses listed below are three credit hour courses, unless otherwise noted. Students pursuing the one-year format must complete the non-thesis track (IST 594). In addition, the one-year M.S. track must adhere to the following conditions:

- Students must take at least one credit of research (IST 594) for each of the three semesters (Fall, Spring, and Summer).
- A research adviser must be assigned to students in their first semester, as selection and discussion of the student's research topic must begin as soon as possible.
- Students who need more time to complete the final paper must be allowed to complete the paper, and have it reviewed and approved after the third semester (Summer) has ended. Students are not required to remain in residence while they complete the final paper. However, extensions granted to students in this program must comply with the Graduate Council policy on deferred grades (https://gradschool.psu.edu/graduate-education-policies/gcac/gcac-400/gcac-401-grading-system/).

These 30 credits are distributed among the following requirements:

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>IST 543</td>
<td>Foundations of Software Security</td>
<td>3</td>
</tr>
<tr>
<td>IST 554</td>
<td>Network Management and Security</td>
<td>3</td>
</tr>
<tr>
<td>IST 815</td>
<td>Foundations of Information Security and Assurance</td>
<td>3</td>
</tr>
<tr>
<td>IST 820</td>
<td>Cybersecurity Analytics</td>
<td>3</td>
</tr>
<tr>
<td>IST 825</td>
<td>Technologies for Web and E-Commerce Application Security</td>
<td>3</td>
</tr>
<tr>
<td>IST 830</td>
<td>Cybersecurity Project Management</td>
<td>3</td>
</tr>
<tr>
<td>Electives</td>
<td>Select 9-12 elective credits from a list available from the program office.</td>
<td>9-12</td>
</tr>
<tr>
<td>Culminating Experience</td>
<td>Choose one of the following:</td>
<td>3</td>
</tr>
<tr>
<td>IST 594</td>
<td>Research Topics (Capstone Project)</td>
<td>3</td>
</tr>
<tr>
<td>IST 894</td>
<td>Capstone Experience (Capstone Course)</td>
<td>3</td>
</tr>
<tr>
<td>Total Credits</td>
<td></td>
<td>33</td>
</tr>
</tbody>
</table>

Minor

A graduate minor is available in any approved graduate major or dual-title program. The default requirements for a graduate minor are stated in Graduate Council policies listed under GCAC-600 Research Degree Policies (http://gradschool.psu.edu/graduate-education-policies/) and GCAC-700 Professional Degree Policies (http://gradschool.psu.edu/graduate-education-policies/), depending on the type of degree the student is pursuing:
• GCAC-611 Minor - Research Doctorate (https://gradschool.psu.edu/graduate-education-policies/gcac/gcac-600/gcac-611-minor-research-doctorate/)
• GCAC-641 Minor - Research Master’s (https://gradschool.psu.edu/graduate-education-policies/gcac/gcac-600/gcac-641-minor-research-masters/)
• GCAC-709 Minor - Professional Doctorate (https://gradschool.psu.edu/graduate-education-policies/gcac/gcac-700/gcac-709-professional-doctoral-minor/)
• GCAC-741 Minor - Professional Master’s (https://gradschool.psu.edu/graduate-education-policies/gcac/gcac-700/gcac-741-masters-minor-professional/)

Student Aid
Refer to the Tuition & Funding (http://gradschool.psu.edu/graduate-funding/) section of The Graduate School’s website. Students in this program are not eligible for graduate assistantships.

World Campus students in graduate degree programs may be eligible for financial aid. Refer to the Tuition and Financial Aid section (http://www.worldcampus.psu.edu/tuition-and-financial-aid/) of the World Campus website for more information.

Courses
Graduate courses carry numbers from 500 to 699 and 800 to 899. Advanced undergraduate courses numbered between 400 and 499 may be used to meet some graduate degree requirements when taken by graduate students. Courses below the 400 level may not. A graduate student may register for or audit these courses in order to make up deficiencies or to fill in gaps in previous education but not to meet requirements for an advanced degree.

Information Sciences and Technology (IST) Course List (https://bulletins.psu.edu/university-course-descriptions/graduate/ist/)

Learning Outcomes
Master of Professional Studies (M.P.S.)
1. [KNOW] Recognize, understand, identify and assess potential threats, vulnerabilities, and consequences in a context from local to global environments.
2. [APPLY/CREATE] Integrate the use of disciplinary methods, techniques, and knowledge to solve practical, real-world problems.
3. [COMMUNICATE] Present scientific evidence and best practice to inform and improve practical, real-world decisions.
4. [THINK] Search, evaluate, and synthesize literature to integrate cyber security principles into disciplines and professional fields.
5. [PROFESSIONAL PRACTICE] Make use of ethical standards and principles of integrity as a foundation in decision-making.

Master of Science (M.S.)
1. [KNOW] Demonstrate breadth and depth of interdisciplinary knowledge and comprehension of the major issues in cybersecurity analytics and operations.
2. [APPLY/CREATE] Use interdisciplinary knowledge and methods of cybersecurity analytics and operations to plan and conduct a research thesis or scholarly paper.
3. [COMMUNICATE] Communicate the major issues of cybersecurity analytics and operations effectively.