Business Cybersecurity Management, M.S.

Degree Offered
• Master of Science in Business Cybersecurity Management

Certificates Offered
• Business Cybersecurity Data Analytics
• Business Cybersecurity Foundations
• Business Cybersecurity Management

Nature of the Program
The M.S. in Business Cybersecurity Management Program is a 12-month or 24-month online program. Students attend an orientation residency and an experiential capstone presentation that corresponds with summer graduation. The online course delivery of this program allows students to work in teams with expert faculty conducting hands-on technical labs, learning complex technologies while working with a flexible schedule and location independence.

This Business Cybersecurity Data Analytics certificate orients both data and technology analysts to the demands and requirements of both securing and analyzing data. The Business Cybersecurity Foundations certificate focuses on the development of a new or overhaul of existing cybersecurity structures in firms of all sizes. The Business Cybersecurity Management certificate prepares students to manage and improve existing cybersecurity programs with an emphasis on the evaluation of risks and where cybersecurity management meets the law.

Although the master’s and certificate programs requires the learning of challenging technical material, entry into the program does not assume or require depth in technology fields. The program is constructed in such a way as to allow students from all backgrounds to get up to speed quickly, while simultaneously challenging those with deep technical expertise.

Academic Standards
In addition to the University’s academic and professional standards, students enrolled in a John Chambers College of Business and Economics master’s degree program must also abide by the following standards:

• Students must have a minimum cumulative GPA of 3.0 to earn a degree from their graduate program, without exception.
  • A student who cannot mathematically meet the 3.0 GPA requirement to successfully complete the degree, within a reasonable period of time (as defined by the Program Coordinator or designee), will be dismissed from their academic program. Visit the Probation, Suspension, and Dismissal section of the University’s Graduate Catalog for more information about this topic.

• Students must follow the professional standards established by their degree program and/or department. A student who violates the established professional standards may be placed on probation, suspended, or dismissed from their program.

• A student whose cumulative GPA falls below 2.75 will automatically be placed on academic probation.
  • A student will be suspended from their program, for up to one year, if their GPA is not raised to 2.75 by the end of their subsequent semester of enrollment. The program will reevaluate the student after the term of suspension to determine whether they may return to the program or be dismissed.

• A student will be suspended from their program if they earn a letter grade below C- in more than one required course.

• A student who earns a letter grade of D or F in any required course must repeat the course and earn a minimum letter grade of C-.
  • Any grade earned in a repeated course at the graduate level is included in the calculation of a student’s overall and major GPA, along with the original grade earned in the course. Additionally, the original grade earned in the course will remain on the student’s academic transcript/permanent record. Visit the Grades section of the University Graduate Catalog for more information about this topic.

Any exceptions to the above standards must be approved in writing by the Associate Dean for Graduate Programs and Global Engagement and the Program Coordinator.

FACULTY
COORDINATOR
• Christopher Ramezan - Ph.D. (West Virginia University)
  Assistant Professor, Management Information Systems
Admissions

The M.S. in Business Cybersecurity Management program seeks individuals from diverse academic backgrounds who have an interest and aptitude to be successful in the cybersecurity domain. This program prepares students to become cybersecurity professionals, as well as sharpen the skills of those who currently work in the cybersecurity industry so that they can adapt to growing changes in security technology.

The Admissions Committee will take a holistic approach to the application review process and will consider the strength of the following admissions application requirements:

- **GPA** - To be competitive, an applicant would present a cumulative undergraduate GPA of 3.25
- **Resume**
- **Statement of Purpose**
- **Letter of Recommendation** - Applicants must have one letter of recommendation from an individual who can provide information about their ability to work with others, discipline and ambition, leadership potential, etc.

The Admissions Committee reviews applications on a rolling basis, and students admitted to the program may begin in the fall or spring semester. Please visit this program's webpage (https://business.wvu.edu/academics/management-information-systems/business-cybersecurity-management/) to learn more about the specific application deadlines and other important information. Students may also contact the John Chambers College of Business and Economics Graduate Programs Office for assistance at (304) 293-5505 or BeGradPrograms@mail.wvu.edu.

Admission Requirements 2023-2024

The Admission Requirements above will be the same for the 2023-2024 Academic Year.

**Major Code:** 2140

*Note* - International Students are required to submit a TOEFL, IELTS, or Duolingo score. The John Chambers College of Business & Economics TOEFL requirement is higher than the University’s—applicants must have a TOEFL-ibt score of 92. If you have taken the IELTS, the minimum score must be 6.5, and the minimum Duolingo score is a 105. English language exam scores should be sent to the Office of Admissions, West Virginia University, PO Box 6009, Morgantown, WV 26506-6009.

All graduate programs in the John Chambers College of Business and Economics require that enrolled students maintain a minimum cumulative GPA of 3.0 in coursework applied toward their degree program, as outlined in the specific academic program of study.

Degree Requirements

Each student who completes an MS in Business Cybersecurity Management will complete a 10 course online sequence in a one year time period. Students are required to attend an on-campus residency and also are required to attend an on-campus residency to present their capstone project at the conclusion of their one year program.

A program GPA of 3.0 is required by the Chambers College.

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBR 510</td>
<td>Cybersecurity Information Systems Management</td>
<td>3</td>
</tr>
<tr>
<td>CYBR 520</td>
<td>Business Cybersecurity Analytics</td>
<td>3</td>
</tr>
<tr>
<td>CYBR 525</td>
<td>Information Security Assurance Management</td>
<td>3</td>
</tr>
<tr>
<td>CYBR 530</td>
<td>Business Data Communications</td>
<td>3</td>
</tr>
<tr>
<td>CYBR 535</td>
<td>Business Network Security</td>
<td>3</td>
</tr>
<tr>
<td>Course Code</td>
<td>Course Title</td>
<td>Hours</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>CYBR 540</td>
<td>Information Ethics and Legal Procedures **</td>
<td>3</td>
</tr>
<tr>
<td>CYBR 545</td>
<td>Business Cybercrime Management</td>
<td>3</td>
</tr>
<tr>
<td>CYBR 550</td>
<td>Business Enterprise Security Architecture</td>
<td>3</td>
</tr>
<tr>
<td>BUDA 550</td>
<td>Business Data Visualization</td>
<td>3</td>
</tr>
<tr>
<td>CYBR 555</td>
<td>Business Cybersecurity Practicum</td>
<td>3</td>
</tr>
</tbody>
</table>

Total Hours: 30

* Students may select CPE 538 in place of the CYBR 535 in the Spring semester, on campus.

** Students may select CS 539 in place of the CYBR 540 in the Spring semester, on campus.

### Suggested Plan of Study - 1 Year

#### First Year

<table>
<thead>
<tr>
<th>Fall Hours</th>
<th>Spring Hours</th>
<th>Summer Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBR 510</td>
<td>CYBR 535</td>
<td>BUDA 550</td>
</tr>
<tr>
<td>CYBR 520</td>
<td>CYBR 540</td>
<td>CYBR 555</td>
</tr>
<tr>
<td>CYBR 525</td>
<td>CYBR 545</td>
<td></td>
</tr>
<tr>
<td>CYBR 530</td>
<td>CYBR 550</td>
<td></td>
</tr>
</tbody>
</table>

Total credit hours: 30

### SPRING START - 18 MONTH

#### First Year

<table>
<thead>
<tr>
<th>Spring Hours</th>
<th>Summer Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBR 535</td>
<td>BUDA 550</td>
</tr>
<tr>
<td>CYBR 540</td>
<td></td>
</tr>
</tbody>
</table>

Total credit hours: 30

### FALL START - 2 YEAR

#### First Year

<table>
<thead>
<tr>
<th>Fall Hours</th>
<th>Spring Hours</th>
<th>Summer Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBR 525</td>
<td>CYBR 535</td>
<td>BUDA 550</td>
</tr>
<tr>
<td>CYBR 530</td>
<td>CYBR 540</td>
<td></td>
</tr>
</tbody>
</table>

Total credit hours: 30

#### Second Year

<table>
<thead>
<tr>
<th>Fall Hours</th>
<th>Spring Hours</th>
<th>Summer Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBR 510</td>
<td>CYBR 545</td>
<td>CYBR 555</td>
</tr>
<tr>
<td>CYBR 520</td>
<td>CYBR 550</td>
<td></td>
</tr>
</tbody>
</table>

Total credit hours: 30
Major Learning Outcomes

BUSINESS CYBERSECURITY MANAGEMENT

Upon completion of this program, students will:

• Students will be able to demonstrate managerial expertise in understanding and investigating complex cybersecurity ideas.
• Students will be able to evaluate the data security of businesses from a data and systems security perspective, and to recommend and initiate appropriate procedures, policies, and security controls to ensure improved data and systems security.
• Students will be able to use appropriate tools to mitigate cybersecurity threats by applying knowledge of topics such as risk management, disaster recovery, business continuity, digital forensics, and computer network defenses.
• Students will be able to communicate the analysis and findings of a comprehensive security audit initiative to enhance the protection and security of an organization.

COURSES

CYBR 510. Cybersecurity Information Systems Management. 3 Hours.
PR or CONC: CYBR 530 or consent made by the CYBR Program Coordinator. Course provides CYBR students an overview of the IT audit function from an information systems administration perspective. This course will examine in detail how to build and manage an effective IT audit operation capable of analyzing, assessing, and evaluating physical, technical, and operational cybersecurity controls using information systems auditing standards and frameworks such as COBIT, ISO, and ITIL.

CYBR 520. Business Cybersecurity Analytics. 3 Hours.
PR or CONC: CYBR 510 or consent made by the CYBR Program Coordinator. Technical and management aspects of building and operating a security operations center (SOC) for an enterprise IT environment. Also focuses on data analysis methods and techniques for analyzing cybersecurity data, as well as an introduction to supervised and unsupervised machine learning/artificial intelligence classification algorithms which can be leveraged to provide insights on data analysis and detection problems in cybersecurity.

CYBR 525. Information Security Assurance Management. 3 Hours.
This course prepares graduate students to become effective leaders in the management of computer security risks and cyber threats in private and public sector organizations. This comprehensive course introduces students to information assurance strategies, managerial security frameworks, the management of security controls, and the protection of information systems and networks in business. Students are also provided with the managerial tools.

CYBR 530. Business Data Communications. 3 Hours.
Provides an overview of corporate data communications networks, the TCP/IP model and related technologies of the data communications corporate infrastructure as well as a survey of the essential tools and strategies for the management of secure, effective business networks. The course focuses on many related areas. Students will be encouraged to take and pass the Network+ Certification.

CYBR 535. Business Network Security. 3 Hours.
PR: CYBR 525 and CYBR 530. This course prepares graduate students to be effective leaders in business network security management. This course focuses on a practical, managerial approach to assessing and maintaining security in organizational networks and private and public cloud infrastructures. The student is expected to learn, think and act as an executive level manager applying network security technologies, controls and policies.

CYBR 540. Information Ethics and Legal Procedures. 3 Hours.
This course provides an introduction to information ethics, including privacy protection and control, surveillance, link analysis, personally identifiable and sensitive data, data anonymity, privacy, accessibility and sharing, censorship, intellectual property, accuracy, virtual reality and AI. Additionally, laws of data collection and storage, security and law enforcement investigations, compliance management for government, publicly held corporations and the healthcare sectors are covered.

CYBR 545. Business Cybercrime Management. 3 Hours.
PR: CYBR 530 and PR or CONC: CYBR 535. Learn the managerial skills to protect, defend, and audit the security of information systems by ensuring confidentiality, integrity, authentications, availability, and non-repudiation through liability assessments, statistical analysis, and risk-based decision making. Upon completion of the course, students should be able to ensure that appropriate business security controls are in place to safeguard digital files and critical electronic infrastructure.

CYBR 550. Business Enterprise Security Architecture. 3 Hours.
PR: CYBR 545 or consent made by the CYBR Program Coordinator. Strategies, techniques, and processes of securing information technology assets through developing and managing an enterprise-wide cybersecurity program that can defend against cyberthreats and risks relevant to modern business enterprise networks and information technology environments. Holistic approach to cybersecurity and emphasizes the development and usage of a comprehensive cyberdefense framework. Introduction into conducting research on current and developing cybersecurity threats.
CYBR 555. Business Cybersecurity Practicum. 3 Hours.
PR: CYBR 545 and PR or CONC: BUDA 550. Students will apply business cybersecurity tools to real world information security issues found in a business or non-profit organization. The final project requires integration across the business cybersecurity management skills of business intelligence, data management, information security assurance, data communications, network security, information ethics, legal procedures, business cybercrime management, fraud data analysis and business data visualization using a holistic approach.

CYBR 591. Advanced Topics. 1-6 Hours.
PR: Consent. Investigation of advanced topics not covered in regularly scheduled courses.

CYBR 593. Special Topics. 1-6 Hours.
A study of contemporary topics selected from recent developments in the field.

CYBR 595. Independent Study. 1-6 Hours.
Faculty supervised study of topics not available through regular course offerings.