CYBERSECURITY

Program Review, November 2025

WILLIAM WOODS
UNIVERSITY

2024 Program Review (2019-2023)

Cybersecurity Studies (BS)

Mission and Introduction

Introduction

1. Provide an overview of the program and the context of where it's housed within the institution (what department, etc.).
2. Discuss any changes in the focus of the program over the cycle of this review.

Narrative:

The Cybersecurity (CSS) program began being offered in the online modality in 2018 and began being offered on-ground in Fall of 2022. The Cybersecurity Major is housed within the School of Business and Technology alongside the Computer Information Systems major for the Undergraduate Technology Programs. In July 2024, Nina McKee became the chair of Undergraduate Technology Programs within the school that oversees this major. Prior to this, Paul Frazier was the program manager for the Cybersecurity program. The only primary change that has occurred over this review cycle has been expanding into the on-ground modality to accompany the online modality for the Cybersecurity major.

Program Mission Statement

1. What changes has the program made to the mission statement over the course of this cycle?
2. Why were these changes made?
3. Are any revisions planned?

Narrative:

No changes have been made to the statement for the Cybersecurity program as it still reflects the mission of the department to prepare students in core knowledge areas of information security. No revisions are planned for the mission statement at this time.

Alignment to Institution Mission

1. How does the mission of the program align with the mission of the institution?

Narrative:

The Cybersecurity Program Mission Statement aligns to the Institution Mission Statement by focusing on professions-oriented education in the form of preparing students for the IT and Cybersecurity workforce, encouraging intellectual inquiry in students through applying skills from core knowledge areas in information security to other career disciplines, and promoting

a student-centered learning environment that supports students in pursuing a career and/or professional graduate education following their time in the program.

Service to the University (Contribution to Campus Climate)

1. What programming and organizational support are offered by the program that benefits the greater student population?
2. Does the program support on-ground/OLC General Education Courses?
3. Highlight any cross listed courses with other programs
4. Highlight any interdisciplinary programming or activities
5. Identify student enrichment programming that could include volunteer opportunities, field trips, workshops… (does not have to be specific to the program, but is beneficial to students on campus)

Narrative:

The program currently supports two General Education classes in both the online and on-ground modalities (CSS 210 - Introduction to Cybersecurity-Q and CIS 102 - Cloud Computing-Q). Both of these courses fall within the Inquiry and Analysis (-Q) section of the general education framework that students complete two courses from. The Cybersecurity department has since offered a field trip to on-ground Cybersecurity majors to attend the STL CyberCon hosted by the University of Missouri-St. Louis each fall following this review period. The WWU department has attended the last two conferences (2023-2024, 2024-2025) and plans to continue offering this opportunity to students annually. The on-ground CSS 210 - Introduction to Cybersecurity-Q course participates in Cybersecurity Awareness Month through students either creating promotional materials like flyers or hosting events. The Cybersecurity department additionally hosts events outside of those developed for Cybersecurity Awareness Month.

Below is the complete list of LEAD events sponsored or co-sponsored by the Cybersecurity Department over the reporting period:

- Escape Room LEAD event (11/10/23)
    1. Developed/planned puzzles for and co-hosted Escape Room for students
- Project: Cyber Shield (10/25/23)
    1. Class Project for CSS 324 – Cybersecurity & Internet Architecture - Cybersecurity class presented a short simulation that represented the importance of cybersecurity hygiene and considering what information is shared online.
- Biometrics and Cybersecurity (10/24/23)
    1. Student Project for CSS 210 – Introduction to Cybersecurity - Group of two students gave a short presentation and activity that described biometrics and its connection to Cybersecurity.
- Benefits of Internships (Cybersecurity Edition) (10/18/23)
    1. Two seniors in the Cybersecurity department presented about the internships they completed.
- Cybersecurity Movie Night (10/10/23)

    1. Student Project for CSS 210 – Introduction to Cybersecurity - Students watched Catch Me If You Can and completed a short survey about Cybersecurity knowledge.
- Cybersecurity Awareness Month Kickoff Party (10/9/23)
    1. Provided a brief overview of Cybersecurity program activities and played Cybersecurity themed board games.
- Murder in the Woods: A Halloween Whodunit (cohosted) (10/27/22)
    1. Criminal justice themed riddles and scavenger hunt hosted to celebrate Halloween
- The Social Engineering Game (October 26, 2022)
    1. Cybersecurity Awareness Month activity/interactive game demonstrating and highlighting tactics used by social engineers in cyber attacks
- Apple Event (September 7, 2022)
    1. Live and encore viewings of the September 2022 Apple Event with reflection form engaging students with the innovations and technologies showcased
- Level Up – Learning Skills for Free (January 26, 2022)
    1. Exploration and overview of free online learning platforms for students (W3Schools, Khan Academy, Microsoft Learn, Duolingo)

The following are courses that are also listed within the Computer Information Systems program:

CIS 102 - Cloud Computing-Q
CIS 225 - Database Management
CIS 250 - Networking
CIS 351 - Project Management
CIS 425 - Enterprise Systems
CIS 450 - Systems Analysis

The following are courses that are also listed within the Criminal Justice program:

CMJ 385 - Digital Evidence and Forensic Investigations
CMJ 440 - Cybercrime and Information Warfare
CMJ 447 - Information Security

Student Learning Outcomes Assessment and Curriculum

Program Student Learning Outcomes and Results

1. Describe how these Outcomes (Objectives) pertain to the program's mission. Have any changes been made to these outcomes over the course of this cycle? Why or why not?

2. Describe the extent to which students in the program have met these outcomes. Include a 5-year picture of the student outcomes with corresponding data that reflect the success or struggles in assessment.

Narrative:

The 6 Program Objectives for the Cybersecurity (CSS) Program are listed below:

- P1 - Discuss the impact of cybersecurity on society and organizations
- P2 - Develop presentations and documentation to communicate technical content.
- P3 - Describe the process of designing a computer system.
- P4 - Design and implement cybersecurity solutions based on a set of requirements.
- P5 - Identify and compare computer networks and architectures.
- P6 - Communicate computer security principles and their application.

The 6 Program Objectives pertain to the program's mission by reinforcing core knowledge areas for securing information and assets (computer networks and architectures, implementation of security controls, cybersecurity best practices) as well as essential soft skills (articulating ideas, communicating information to different audiences) used within the field that are needed to be successful when entering the workforce or pursuing graduate education. No changes have been made to these outcomes over the course of this cycle as they still align to the program's mission and to the skills students will need beyond their time in the program.

Below are the program objective student outcomes with supporting data for the Cybersecurity Program:

Cybersecurity Studies (BS)_2024-2025 Curriculum and Assessment Findings_2024-2025 (Program Objectives 3, 5, 6 MET | Program Objectives 1, 2, 4 NOT MET)

2021-2024 Data (These assessed courses were not offered / no data was collected before this point)

Encryption Techniques 2019-2023 Data (Encryption Techniques - Objectives 4 and 6 | 2021-2022 MET | 2022-2023 MET | 2023-2024 NOT MET)

Social Engineering 2019-2023 Data (Social Engineering - Objectives 1 and 4 | 2021-2022 MET | 2022-2023 MET | 2023-2024 MET)

Cybersecurity Capstone 2019-2023 Data (Cybersecurity Capstone - Objectives 1, 2, 3, 4, 5, and 6 | 2021-2022 MET | 2022-2023 MET | 2023-2024 NOT MET)

Final Research Study (Cybersecurity Independent Study - Objective 2 | 2019-2023 NOT MET. Data was not collected due to inconsistent rotations as it's only offered on an as-needed basis and not every student takes this class since they have an option between this and CSS 451/CSS 452 Internship for their experiential learning requirement)

For years/terms where some of these objectives were not met (at least 80% of students completing an assessed activity for a particular year did not score at least 75% or above on the assignment), there are some instances where the activity was not completed at all by individual students leading to some outliers that brought down the average with some of the smaller class sizes early on in the program's existence.

Evidence:

- Cybersecurity Annual Assessment 2019-2020
- Cybersecurity Annual Assessment 2020-2021
- Cybersecurity Annual Assessment 2021-2022
- Cybersecurity Annual Assessment 2022-2023
- Cybersecurity Annual Assessment 2023-2024
- Cybersecurity Capstone 2019-2023 Data
- Cybersecurity Studies (BS)_2024-2025 Curriculum and Assessment Findings_2024-2025
- Encryption Techniques 2019-2023 Data
- Social Engineering 2019-2023 Data

Assessment Measures

1. Discuss the measures (rubric evaluation - tool used to gather information) you've selected or developed to measure for each Outcome (Objective).
2. Why were these measures chosen?
3. Were any measures or assessment instruments changed over the course of this cycle? Why or why not?
4. Note any action items related to assessment measures that will be changed moving forward due to the review of assessment data.

Narrative:

Below are the program objectives/outcomes utilized throughout the review cycle:

- P1. Discuss the impact of cybersecurity on society and organizations.
- P2. Develop presentations and documentation to communicate technical content.
- P3. Describe the process of designing a computer system.
- P4. Design and implement cybersecurity solutions based on a set of requirements.
- P5. Identify and compare computer networks and architectures.
- P6. Communicate computer security principles and their application.

The measures and assessment instruments chosen at the beginning of the review cycle were not changed during the review cycle. The measures/rubric evaluation tools used to gather information included the following:

- CSS 401 - Encryption Techniques Case Study Paper (Objectives 4, 6)
- CSS 410 - Social Engineering Case Study (Objectives 1, 4)
- CSS 490 - Cybersecurity Capstone CISO Whitepaper Project Plan (Objectives 1, 2, 3, 4, 5, 6)
- CSS 300 - Independent Study Final Research Study (Objective 2)

Each of these to be assessed at 80% of students scoring at least 75% or higher on the assignments listed above. These assignments were chosen to assess the objectives as they

required students to implement cybersecurity best practices related to the course's primary topics, reinforced soft skills like developing documentation and articulating ideas, and also encourages students to think about the impacts of cybersecurity from multiple perspectives.

For the next review cycle, the following changes are planned for the assessment measures used for the program:

- Refine rubrics for the CSS 401 - Encryption Techniques, CSS 410 - Social Engineering, and CSS 490 - Cybersecurity Capstone courses that allow for a more streamlined approach to gathering this assessment data and creating more consistency among the on-ground and online version of the CSS 490 course for assessment.
- Replace the CSS 300 - Independent Study measure with a different core course as data was not able to be readily and consistently collected due to the inconsistent rotations for this course (only offered on an as-needed basis) and not every student takes this class since they have an option between this and CSS 451/CSS 452 Internship for their experiential learning requirement.
- Ensure every objective is assessed at least twice in the program (currently Objective 3 and 5 are only assessed once).
- Potentially introduce an entrance/exit exam for the program that addresses some of the above action items related to assessing objectives.

Evidence:

- Cybersecurity Studies (BS)_2024-2025 Curriculum and Assessment Findings_2024-2025

Curriculum Map

1. Highlighting any key or core courses, have any changes been made to this pathway or degree requirements over the course of this cycle? (Upload Program Checklist)
2. Why or why not?
3. Explain how the program sequence of courses is designed and why it is laid out in that way? (scaffolding)

Narrative:

Key courses related to assessment for the Cybersecurity Program include CSS 401 - Encryption Techniques, CSS 410 - Social Engineering, and CSS 490 - Cybersecurity Capstone. CSS 210 - Introduction to Cybersecurity-Q and CIS 250 - Networking are pre-requisite courses for all of the 300/400 level CSS courses in the program. No changes have been made to the pathway or degree requirements over the course of this cycle. (Note: Some courses have changed course code prefixes/numbers from MIS to CIS though the courses themselves are the same).

Students take primarily 100 and 200-level courses when they begin the program focusing on fundamentals such as Introduction to Cybersecurity, Networking, Database Management, Cloud Computing. Later on in the program, students take primarily 300 and 400-level courses that focus on Cybersecurity & Internet Architecture, Cyber Attacks and Defenses, Cybersecurity Law & Ethics, Social Engineering, Encryption Techniques, Information Security, and Cybercrime and Information Warfare. Course sequences are largely informed by course rotations and for on-ground students, the classes that are only offered online are spread out across semesters whenever possible to stagger them and provide a balance of in-person and online classes.

Cybersecurity Program Checklist

Evidence:

- Cybersecurity Program Checklist

Concentrations

1. If the program has concentrations, please upload the concentration data.
2. Speak to the enrollment distribution of students within the concentrations and any impact on course rotation.
3. Include strategies or processes for retention and recruitment within the concentration.
4. Explain the value of each concentration and how they enhance the skills students need to be successful in the field.

Narrative:

N/A

This program does not have concentrations.

Course Descriptions

1. Highlight any changes to course descriptions that have occurred over the identified timeframe. (upload a pdf of the course descriptions)

Narrative:

No changes have occurred to course descriptions over the review cycle. Below is the list of course descriptions for the Cybersecurity Program:

Cybersecurity Program Course Descriptions

Evidence:

- Cybersecurity Program Course Descriptions

Curriculum Delivery

1. Does online enrollment impact enrollment in the campus enrollment?
2. If the program has an online component, explain how the program coordinates schedules and curriculum between the two modalities.

Narrative:

Online enrollment has not adversely affected on-campus enrollment in Cybersecurity courses. When advising for on-ground students occurs, the primary academic advisor advises students into the on-ground sections of the Cybersecurity major courses unless there is a specific conflict that prevents a student from taking the course at that specific time. Students who are on-campus then take the remaining courses that are not offered on-ground in the online offerings. These online courses are scheduled during advising sessions to try and spread them out throughout multiple semesters during a student's progression through the program. The curriculum is divided up based on the expertise of the faculty teaching in the program.

Below is the breakdown of course modalities for the program.

Courses that are offered in **both** online and on-ground modalities include the following:

CMJ 440 - Cybercrime and Information Warfare
CIS 225 - Database Management Systems
CIS 250 - Networking
CIS 351 - Project Management
CIS 425 - Enterprise Systems
CIS 450 - Systems Analysis
CSS 210 - Introduction to Cybersecurity-Q
CSS 324 - Cybersecurity & Internet Architecture
CSS 325 - Cyber Attacks and Defenses
CSS 440 - Cloud Security
CSS 490 - Cybersecurity Capstone

CSS 300 - Independent Study
CSS 451/452 - Cybersecurity Internship I/II

Courses that are **only offered online** include the following:

CMJ 385 - Digital Evidence and Forensic Investigations
CMJ 447 - Information Security
CIS 102 - Cloud Computing-Q
CSS 310 - Cybersecurity Law & Ethics
CSS 401 - Encryption Techniques
CSS 410 - Social Engineering
CSS 420 - Critical Infrastructures

Participation in Assessment

1. Discuss faculty participation in program assessment
2. How involved are faculty and what is their responsibility for the assessment of the program.

Narrative:

Following this review period, online courses were modified to run in 5-week sub-terms. Faculty members assisting with this transition were provided a course writing toolkit. Within the course writing toolkit that faculty/course writers were provided and during the Microsoft Teams small group meetings held to support faculty in being able to facilitate the new format of online classes (a shift from 8 weeks to 5 weeks), notes for courses being assessed were provided so that they were aware which objectives were mapped to their course(s). The faculty members writing/revising the courses that had an assessment component were included in the discussion with the program chair on which assignment/project best aligned to the objective being assessed.

Going forward, there are plans for the program chair to provide some brief virtual trainings to faculty members facilitating these courses on how to use the rubrics in either Watermark/Student Learning & Licensure or BrightSpace to continue to ensure consistent and accurate data is collected.

Action Items and Use of Results

1. Summarize or highlight action items taken as a result of program's assessment results.
2. How have the results driven improvement over the course of this cycle?

Narrative:

For the next review cycle, the following action items are planned based on improvements the program seeks to make based on the data that was collected during this cycle:

- Revise Measurements/Assessments for Courses
    - Refine rubrics for the CSS 401 - Encryption Techniques, CSS 410 - Social Engineering, and CSS 490 - Cybersecurity Capstone courses that allow for a more streamlined approach to gathering this assessment data and creating more consistency among the on-ground and online version of the CSS 490 course for assessment.
    - Replace the CSS 300 - Independent Study measure with a different core course as data was not able to be readily and consistently collected due to the inconsistent rotations for this course (only offered on an as-needed basis) and not every student takes this class since they have an option between this and CSS 451/CSS 452 Internship for their experiential learning requirement.

- Gather Additional Data
    - Ensure every objective is assessed at least twice in the program (currently Objective 3 and 5 are only assessed once).
    - Potentially introduce an entrance/exit exam for the program that addresses some of the above action items related to assessing objectives.
    - With increased enrollment in courses in both modalities, continue to collect more data throughout the entire review cycle now that the program is established.

Evidence:

- Cybersecurity Studies (BS)_2024-2025 Curriculum and Assessment Findings_2024-2025

General Education

1. • How does program coursework expand on the skills learned in General Education curriculum?

Narrative:

Below discusses the new general education framework that was being discussed/implemented during the review cycle. (Note: Some courses changed course codes from MIS to CIS):

The following courses are aligned to the Inquiry and Analysis (-Q) section of the general education framework and are offered as general education courses that was being voted upon/implemented during the review period:

CSS 210 - Introduction to Cybersecurity
CIS 102 - Cloud Computing

The following courses have a strong written component to them (case study responses, reports, research papers) that build upon the writing fundamentals developed in the Written Communication general education courses:

- CIS 351 - Project Management
- CSS 401 - Encryption Techniques
- CSS 410 - Social Engineering
- CSS 490 - Cybersecurity Capstone

The following courses have a strong numerical component to them (arithmetic with functions, aggregation of data, binary to hexadecimal conversions, etc.) that build upon the mathematics fundamentals developed in the Mathematics general education courses:

- CIS 225 - Database Management Systems
- CIS 250 - Networking

The following courses encourage students to continue exploring issues, objects, or works through the collection and analysis of evidence to make informed conclusions or judgments (often through applying cybersecurity best practices to various systems, contexts, and scenarios) that build upon the fundamentals established in the Inquiry and Analysis designated courses:

- CIS 425 - Enterprise Systems
- CIS 450 - Systems Analysis

- CMJ 385 - Digital Evidence and Forensic Investigations
- CMJ 440 - Cybercrime and Information Warfare
- CMJ 447 - Information Security
- CSS 324 - Cybersecurity & Internet Architecture
- CSS 325 - Cyber Attacks and Defenses
- CSS 440 - Cloud Security

Below discusses the alignment of courses and program objectives to the general education framework used in the beginning of this review period:

CSS.1: Discuss the impact of cybersecurity on society and organizations. (Aligns with the General Education Cluster: Critical Analysis, Society and the Individual).

CSS.2: Develop presentations and documentation to communicate technical content. (Aligns with the General Education Cluster: Creative Expression).

CSS.3: Describe the process of designing a computer system. (Aligns with the General Education Cluster: Quantitative Inquiry).

CSS.4: Design and implement cybersecurity solutions based on a set of requirements. (Aligns with the General Education Cluster: Quantitative Inquiry).

CSS.5: Identify and compare computer networks and architectures. (Aligns with the General Education Cluster: Quantitative Inquiry).

CSS.6: Communicate computer security principles and their application. (Aligns with the General Education Cluster: Creative Expression).

Courses in the program that build upon the skills learned in general education courses include:

CMJ 385 Digital Evidence and Forensic Investigations: Quantitative Inquiry

CMJ 440 Cybercrime and Information Warfare: Quantitative Inquiry

CMJ 447 Information Security: Quantitative Inquiry

CSS 210-Introduction to Cybersecurity: Critical Analysis, Creative Expression, Quantitative Inquiry

CSS 310 Cybersecurity Law & Ethics: Critical Analysis, Society and the Individual

CSS 324 Cybersecurity & Internet Architecture: Quantitative Inquiry

CSS 325 Cyber Attacks and Defenses: Quantitative Inquiry

CSS 401 Encryption Techniques: Quantitative Inquiry

CSS 410 Social Engineering: Quantitative Inquiry

CSS 420 Critical Infrastructures: Quantitative Inquiry

CSS 440 Cloud Security: Quantitative Inquiry

CSS 490 Cybersecurity Capstone: Critical Analysis, Creative Expression, Quantitative Inquiry

MIS 100 Cloud Computing: Quantitative Inquiry

MIS 225 Database Management Systems: Quantitative Inquiry

MIS 250 Networking: Quantitative Inquiry

MIS 350 Project Management: Quantitative Inquiry

MIS 425 Enterprise Systems Quantitative Inquiry

MIS 450 Systems Analysis: Quantitative Inquiry

Faculty Qualifications, Activities and Scholarship

Faculty Specialization

1. Discuss the scholarship and research content of the faculty in the program, being sure what their specialization brings to the program.
2. Explain the core features of the program based on the current faculty.
3. How could the program be expanded (new courses, areas of specialization, etc.)?
4. How might additional instructional members allow the program to expand and/or change the focus of the program curriculum?

Narrative:

Below are the faculty members for the Cybersecurity program with their primary areas of teaching/scholarship as well as experience they bring to the program:

(Full-Time/On-Ground Faculty)
Nina McKee - Networking, Database Management, Project Management, Cybersecurity & Internet Architecture, Cyber Attacks and Defenses, Introduction to Cybersecurity, Cloud Security, Enterprise Systems, Systems Analysis, Cybersecurity Capstone

- Master of Science in Cybersecurity from Maryville University
- Master of Business Administration (MBA) from William Woods University

(Online Adjunct Faculty)

Paul Frazier - Social Engineering, Independent Study Projects

- Master of Science in Systems Management from University of Southern California
- Over three decades of military, teaching, and consulting experience related to Cybersecurity including roles as Cybersecurity Engineer with the U.S. Transportation Command, Information Assurance Engineer and Division Chief with the Air Force Network Integration Center

Dr. Ihsaan Alkadi - Encryption Techniques

- Ph.D. in Computer Science from Louisiana State University
- Previously authored a book titled "A New Technical and Practical Approach on Securing Cyberspace and Cloud Computing"
- CompTIA Security+ Certification

Bree Perdun - Cloud Security, Cybersecurity Capstone

- M.A. Information Technology Management from Webster University
- Extensive industry and military experience as IT Operations Analyst for the National Geospatial Intelligence Agency, Electronic Security Systems Operator for the United States Air Force, and Cyber Security Operations Specialist for NJVC

John Tierney - Critical Infrastructures

- MA, National Security and Strategic Planning, Naval War College
- 35 years of professional experience including roles as Associate for Booz Allen Hamilton, Senior Functional Analyst for Dynamics Research Corporation, and Senior Member of the Professional Staff for SRA International

Mark Dalle - Cybersecurity & Internet Architecture, Cyber Attacks and Defenses, Cybersecurity Law & Ethics

- MA, Computer Resource/Information Management from Webster University
- Extensive industry and military experience including roles as IT Specialist — Air Force Network Integration Center and Principle Security Engineer, Security Test & Evaluation Engineer, Information Assurance Analyst — EADS

Todd Larivee - Project Management, Introduction to Cybersecurity

- Certified Information Systems Security Professional (CISSP) Certification
- Extensive industry experiences including roles as Director Analyst for Endpoint Management and Desktop Virtualization at Gartner and IT Security and Technology Section Chief at the Missouri Department of Conservation

Ron Martin - Networking, Enterprise Systems, Systems Analysis, Database Management

- Master of Business Administration (MBA) form Fontbonne University
- Over a decade of industry experience in roles pertaining to project management, system administration, network engineering, and IT management

Steffany Tinnin - Introduction to Cybersecurity

- Certified Scrum Master (CSM), Scrum Alliance
- GIAC Security Leadership Certification (GSLC), SANS, DoD 8570 Level III
- Professional Continuity Practitioner (PCP) Level 1, FEMA
- Experience as Cybersecurity Risk Management, Team Lead for the National Geospatial Intelligence Agency (NGA)

Hilary Bainbridge - Cloud Computing

- Master of Science in Human Computer Interaction (HCI) from Iowa State University
- Master of Business Administration (MBA) from William Woods University
- 10+ Years in UX Research, UX Design, and Quality Assurance roles

Additional instructional members would allow the program to expand on-ground course rotations and eventually incorporate additional specializations in areas like Penetration Testing/Ethical Hacking, Security Information and Event Management (SIEM) systems, and Security Operations Centers (SOC).

Faculty Awards and Honors

1. Discuss and highlight awards and honors received by faculty over the course of the cycle.

Narrative:

Below are the awards and honors received by faculty over the review cycle:

- Todd Larivee
  - Earned the Certified Information Systems Security Professional (CISSP) Certification

- Dr. Ihssan Alkadi
  - Earned the CompTIA Security+ Certification

Faculty Workload

1. Summarize the workload and responsibilities of faculty.
2. What actions are you taking to avoid faculty overload?
3. % of course load is taught by program faculty vs adjunct
4. % of courses covered by full time faculty
5. % of courses covered through faculty overload

Narrative:

The Cybersecurity program courses were primarily taught by 1 full-time on-ground faculty member and 9 online adjunct faculty members during the review period.

79/102 courses or 77% of courses were taught by online adjuncts during the review period. (Note: The program was primarily only offered on-ground until Fall 2022 with some MIS/CIS

courses offered on-ground before that point).

23/102 or 23% of courses were taught by on-ground full-time faculty during the review period. (Note: There were no on-ground adjuncts for the program during this review period (100% of on-ground courses taught by full-time faculty). Additionally, there were no overloads during the review period due to low enrollment in courses).

During and beyond this review cycle, actions taken to avoid faculty overload include advising on-ground students into on-ground sections of courses with the minimum number of students needed to be considered a full class based on course rotations to avoid extra tutorial sections of core courses. Independent Study and Internship Courses are also distributed amongst on ground and online faculty members.

Faculty Workload Data for Cybersecurity Assessment

Evidence:

- Faculty Workload Data for Cybersecurity Assessment

Program Data: Student Experience

Enrollment and Recruitment

1. What are the trends with enrollment in this program over the course of the review cycle?
2. How does this compare to institutional trends or similar programs on campus?
3. Describe recruitment efforts or goals such as increased enrollment or diversity.
4. Have these initiatives been successful?

Narrative:

Trends with enrollment in the Cybersecurity program have been largely positive over the review cycle for both on-ground and online modalities. The Cybersecurity department had 9 total students in the program in Fall 2019 with an increase to 12 and 15 in Fall 2021 and Fall 2022, respectively. The largest growth in enrollment occurred going into Fall 2023 with a total enrollment of 52 students (39 online, 13 on-ground) for the program.

One of the initiatives that drove this increased enrollment was the implementation of Woods Global which emphasized the online modality of this program as well as other programs across campus. This initiative was a great success for the Cybersecurity program that increased online enrollment from 9 students in Fall 2022 to 39 students in Fall 2023. Additionally, the on-ground modality had 6 students when the first CSS 210 - Introduction to Cybersecurity-Q course was offered on campus and has since grown to 19 on-ground students as of Fall 2024.

Cyber Program activity

Evidence:

- Cyber Program activity

Retention

1. Has student retention remained in an acceptable range over the course of the review cycle?
2. What strategies are program faculty using to raise retention rates within the program?

Narrative:

Student retention has remained in an acceptable range over the course of the review cycle. The Fall-to-Fall Retention rate of First-Time Full-Time Freshmen for Fall 2019-2020, Fall 2020-2021, Fall 2021-2022, and Fall 2022-2023 has been 100%. (For each of these years 1 to 3 students met the definition of First-Time Full-Time Freshmen). The retention rate only decreased for Fall 2023-2024 (66.6%) with 1 student that did not return. All of the other students retained within the University, within the Department, and within the Major.

Strategies used to maintain and raise these retention rates include offering program-specific faculty and student tutors through the Academic Success Center on campus, hosting campus engagement activities such as Cybersecurity Awareness Month events, and fostering networking opportunities amongst online and on-ground Cybersecurity students with dedicated LinkedIn profile development activities built into courses to encourage students to populate their profiles and follow their peers and industry professionals on the platform.

Curriculum/Course Retention and Success

1. Describe enrollment trends in the courses within the program. (upload course enrollment spreadsheet)

2. Reflect on the success of the students within the courses over the designated time frame.
- Highlight some completion or withdrawal and failure rates in the core courses.
- Were these in line with expectations? (we will need to provide this data)

3. For programs with dual modalities, reflect on the success of students within the courses over the designated time frame.
- Highlight some completion or withdrawal and failure rates in the core courses.
- Were these in line with expectations? (we will need to provide this data)

Narrative:

Enrollment within the Cybersecurity program courses has maintained or trended upwards over the review cycle for both online and on-ground courses. Some notable course enrollment increases include Cloud Computing OLC (7 enrollments for Fall 2021, and 6 enrollments for Spring 2023 increasing to 17, 21, and 25 enrollments for Summer 2023, Spring 2024, and Summer 2024, respectively) as well as CMJ 385 OLC (5 enrollments in Summer 2023 increasing to 13 enrollments in Fall 2023 and the 20 enrollments in Summer 2024). Some smaller course enrollments occurred during the review cycle for students who needed tutorial classes to fulfill requirements ahead of graduation.

Students within these courses have overall performed successfully within these courses and there were in line with expectations. Some failure and withdrawal percentages per year trend a bit higher in the earlier part of the review cycle when fewer students were enrolled in these courses. Failure and withdrawal rates are similar when comparing online and on-ground modalities for core Cybersecurity courses at around 6% or less. A couple core courses that saw some higher rates were CSS 210 - Introduction to Cybersecurity (30.77% failure rate for one sub-term in 2023-2024 and 17.86% failure rate for one sub-term in 2024-2025) and CSS 420 (25% failure rate in 2021-2022 though this section only had 4 enrollments). CSS 210 has run multiple additional sections compared to other courses due to being a general education course and a pre-requisite for other upper-level CSS courses.

Cyber Enrollment 2019-2024

CSS Course Grade Report

Evidence:

- CSS Course Grade Report
- Cyber Enrollment 2019-2024

Completion

1. How many students are graduating from the program?
Have the completion rates been in line with expectations?

2. Describe findings resulting from exit surveys or program alumni surveys that were conducted over the course of the cycle. (programs will need to do annual exit surveys to capture this data)

Narrative:

In total for the review cycle (2018-2019 to 2022-2023 academic years), 6 students graduated from the Cybersecurity program. These students were all online as the on-ground classes started being offered in Fall 2022. December 2020 was when the first student graduated as the program was established in 2018. After this review cycle (later in Summer 2023 and in 2024 and 2025) additional online students as well as on-ground students (7 in total across both modalities) have graduated from the program. These completion rates have been in line with expectations based on enrollment and the number of completions are anticipated to increase with the increased enrollment the program has seen. No Exit Surveys have been collected as of this review cycle.

Cybersecurity Completion Data 2020-2025

Evidence:

- Cybersecurity Completion Data 2020-2025

Course Evaluation Data

1. What were some positive and negative feedback received from students who completed the courses?
2. Highlight any trends or insights that came from course evaluations over the course of the cycle. (data will have to be available)

Narrative:

Feedback provided on end-of-course evaluations by students was largely positive for classes across on-ground and online modalities. Students consistently noted the clear instruction provided by faculty, availability of instructors and resources, and overall enjoyment of the content and presentation of materials within courses. Some critiques from students included certain online learning platforms they preferred or did not prefer, a couple opportunities for additional interactive activities in courses, and a couple suggestions for pacing of certain assignments (introducing final projects earlier in some courses, etc.). Some of these concerns have already been addressed throughout the transition to the 5-week sub-terms and the opportunity it presented to refresh the curriculum.

As evidenced by the data linked below for the Cybersecurity Core End of Course evaluations, scores for both on-ground and online modalities were consistently in the range of 4.3 to 4.9 which is near or in some cases above the University averages for these 8 question categories.

Cyber Security

Evidence:

- Cyber Security

Student Advising

1. Describe the advising process for your program?
2. What strategies and structures are in place to facilitate a successful advising period?
3. What is the optimal ratio of advisees to adviser for the program?
4. Explain any other processes to increase the effectiveness of the current advising procedure.

Narrative:

For online students, advising is completed by on-campus advisors and not by faculty. On-ground students who have declared the Cybersecurity major were assigned to Nina McKee during the review period and the incoming students for the next academic year will work with Nina McKee as the primary academic advisor for this major. Students will take a combination of online and on-ground classes based on course rotations and modality chosen for the program. The optimal ratio of advisees to adviser ratio for the program is 25-30 students. This is manageable as many of the on-ground course rotations occur a couple of times within a student's time in the program making many degree plans very consistently structured as far as when core courses are taken by students. For on-ground students, an advising toolkit with

resources as well as an Excel template are being developed to assist with this process.

Student Awards and Achievements

1. Highlight the accomplishments and external honors received by students in the program over the course of this cycle.

Narrative:

No student awards to report during the specific review period. Directly following this timeframe, the achievement below occurred:

William Woods University 2024 Symposium for Scholarship, Research, and Creativity | April 11, 2024
CSS 490 – Cybersecurity Capstone Project | Sandbox Sentinel: Building the Ultimate Malware Playground

This project consisted of a researched development plan and proposal for a malware sandboxing environment for testing and learning about different types of malicious software. The project included planning and outlining all implementation phases including the following - a network map of the sandbox, software to be included, defined experiential learning opportunities within the Cybersecurity curriculum, and what hardware would be needed to maintain this environment.

Senior Capstone Group (2 Student Presenters) selected to be one of six presenting groups at the competitive Outstanding Senior Showcase

Clubs and Co-Curricular

1. Does your program support any clubs and co-curricular activities that contribute to positive student experiences?
2. How does this contribute to the program?
3. To the campus experience of students?

Narrative:

The primary co-curricular activity offered to students following this review cycle is an annual field trip to attend the STL CyberCon Cybersecurity conference hosted by the University of Missouri-St. Louis each fall. This conference consists of sessions hosted by companies like Mastercard, Netskope, and Google and also includes a Cybersecurity-focused career fair. This event provides a valuable networking opportunity for students as well as an opportunity to discover internships and jobs within the discipline.

At this time the program does not support any clubs/organizations.

Program Analysis

SWOT Analysis

1. Strengths, Weaknesses, Opportunities, and Threats.

Narrative:

Strengths

- Coursera integration in the program with the IBM Cybersecurity Analyst Professional Certificate
- Focus on experiential learning with an internship or independent study project completed by each student
- Annual field trip offered to on-ground students to the STL CyberCon hosted by the University of Missouri-St. Louis
- Students present each year in the William Woods Symposium for Research, Scholarship, and Creativity

Weaknesses

- No on-campus internship opportunities at this time
- Currently no Cyber Range actively offered/in use for virtual labs/activities

Opportunities

- Program offers classes that overlap with the topics covered in the Master of Science in Business Analytics Program that make it a great option for students to continue their education at William Woods
- Online courses offered in 5-week sub-terms year-round that allow students to expedite degree completion / help transfer students stay on track for anticipated graduation dates

Threats

- Updates to Coursera content/certificate that could affect micro-course mapping to current Cybersecurity classes
- Rapidly evolving industry that requires curriculum to be reviewed often to keep information relevant and updated
- Costs of certain industry tools or conferences eventually creating budget expenses or additional expenses for students for course materials

Campus Facility and Resources

1. Provide an analysis on how adequate the spaces that are most used by the program on campus (laboratories, office space, classrooms/LMS, etc.).

2. Please discuss any updates or modifications to the facility or resources available to the program that have impacted student learning.

3. Recommendations to Improve Facilities and Resources

Narrative:

Over the review cycle, the Cybersecurity program has added a dedicated on-campus computer lab for all of the on-ground Cybersecurity courses to be held in. This has been a tremendous asset in ensuring students can access platforms and in-class activities that require certain software and/or web-based applications if students do not utilize a personal device. The computer lab has been able to support the course load needs of the on-ground rotations with 15 workstations.

The on-ground Cybersecurity instructor's office has moved from the top floor of the Burton building to the main floor of the Burton building to be right next to the dedicated computer lab. Additionally, this new office space is larger and can be utilized to facilitate small group projects if specialized technology needs to be secured in a locked facility when not in use.

Recommendations for further improvements in facilities and resources would include having a segmented/isolated network for the computer lab to allow for more experiential projects and activities to occur in certain courses while ensuring that the enterprise network is not affected. Additionally, having dedicated virtual machines and/or access to a cyber range would allow for authentic simulations of cyber attacks and defense methods for students to gain experience utilizing industry tools.

Library Report

* Upload the Library report provided by the University Library

1. Please describe the usage of library resources.
2. How do faculty and students feel the library meets the program's needs?

Narrative:

Faculty and students are happy with the library's current selection of resources for cybersecurity and related topics. Currently a combination of print and digital materials are available to be used by both faculty and students.

From the collection provided, 94 titles were accessed during this review period. Some of the most common subjects searched included artificial intelligence, cloud computing, computer security, and big data.

The most frequented journals include the International Journal of Information Security, Journal of Computer Security, Computerworld, International Review of Law, Computers &

Technology and International Journal of Information Security Science.

Potential areas of expansion for the Library's collections related to cybersecurity could include obtaining a digital subscription to the IEEE *Xplore* Digital Library. The Library Director is currently getting a price quote for the service and will see if it fits into the library budget.

The library report can be found linked below:

Library Collection Analysis -- Cybersecurity 2025

Evidence:

- Library Collection Analysis -- Cybersecurity 2025

Cost Analysis

1. What was the annual budget for the program for the past 5 years?
2. How was the budget spent? (breakdown of budget expenses)

Narrative:

Below are the annual budgets for each of the years for the program during this review cycle:

Cost Breakdown Per Academic Year
Amount Spent - Total Annual Budget - Amount Remaining - Percentage of Budget Spent

2020-2021

$2.79	$500.00	$497.21	0.56%

2021-2022

$205.34	$1,000.00	$794.66	20.53%

2022-2023

-	1,000.00	0.00%

Note: During part of this review cycle, the Cybersecurity budget was combined with the Management Information Systems (MIS) program budget as the MIS program was being sunset, and certain classes were still being offered in the catalog.

The primary expenses were duplication fees and GoDaddy website hosting for a website development course that was a part of the Management Information Systems program and being taught on-ground during this review cycle.

The dedicated Cybersecurity full-time faculty member's first full academic year was at the end of this review cycle (2022-2023). Prior to this there was a full-time MIS faculty member that taught MIS/CIS courses within the Cybersecurity program. Following this, Cybersecurity budget expenses consisted of taking students to attend the STL CyberCon (food, gas, bus driver), Raspberry Pi devices, and books that utilized a larger percentage of the annual budget.

Specialty Accreditation

Does the program hold specialty accreditation?

If yes, please include the name of the accrediting body and upload the most recent accreditation letter. (description of the data points – describe the accreditation cycle– identify any points of concern noted on the most recent accreditation)

Narrative:

At this time the program does not hold specialty accreditation.

Paul Frazier aligned the program to meet National Security Agency's (NSA) accreditation through their National Centers of Academic Excellence program. Additional data is needed (minimum of at least one complete cycle of on-ground students completing the program) before the program can pursue this accreditation.

Industry and Program Trends

Analysis of the Discipline

1. Provide context for the status of the discipline today.
2. What are some emerging trends in this discipline across the country?
3. What is happening in the industries related to this discipline?

Narrative:

The state of Cybersecurity (and technology overall) is constantly and rapidly evolving. As technology advances, so do the threats that organizations and individuals face to the security of their data and other critical assets, systems, and infrastructures. As such, those in the cybersecurity discipline must also continue to adapt and evolve to address these challenges. Some emerging trends within the discipline include advanced persistent threats and cyber attacks that are larger in scope being more prevalent, ransomware becoming more difficult to evade, zero trust architectures (proving that someone should have authorized access to certain information even if they are already within a network) becoming more common across industries, and quantum computing's effects on cybersecurity.

Quantum computers use qubits rather than bits (what classical computing uses) which enable them to perform calculations simultaneously and much more quickly rather than sequentially which occurs with classical computing. According to Siddiqui (2025), "Once quantum computers reach a certain level of power, they'll be able to break the 2048-bit public key encryption we rely on to protect our data. That might sound far off, but IBM predicts it could happen by the late 2030s." Continued adaptation of existing and emerging technologies such as Artificial Intelligence, Machine Learning, and Cloud Computing will also

inform the cybersecurity landscape's threats and security controls.

References

Siddiqui, L. (2025, May 19). *Top cybersecurity trends in 2025: 9 trends to watch*. Splunk. https://www.splunk.com/en_us/blog/learn/cybersecurity-trends.html

Comparison to Similar Programs at Peer Institutions

1. Identify and discuss how similar programs compare to your program in terms of size, curriculum and any relevant attributes.

Narrative:

Nearby institutions (Maryville University and Lindenwood University in St. Louis and St. Charles, respectively) have larger enrollment and thus more degree completions as of 2023 than the William Woods Cybersecurity program. (Bachelor's Degree Completions: Maryville - 78 students, Lindenwood - 18 students, William Woods - 3 students (Lightcast, 2023)).

The Maryville University Cybersecurity program was established in 2014 (MPress, 2024) and the Lindenwood University IT programs were overhauled to include Cybersecurity in 2019 and 2020 (CyberSecurityDegree.com, 2022). The William Woods program has grown within this review cycle and is projected to see even more growth which will contribute to an increased number of degree completions as the program becomes more established like the other institutions.

The Maryville University Cybersecurity program offers tracks of courses including Defensive Security, Offensive Security, and General track along with a Cybersecurity core and a Business core. (Maryville University, 2023). Some of the unique courses within these tracks include mobile security, security information & event management, ethical hacking, and an experiential Security Operations Center (SOC) where students work with clients. Maryville also offers online virtual machines for certain courses through their Maryville Open Lab.

The Lindenwood Cybersecurity program's courses primarily exist within a core set of classes. Some of the unique courses offered there include Blockchain Technology for Business, Advanced Penetration Testing, and Web Based Application Security. (Lindenwood University Online, 2025). Lindenwood's Cybersecurity programs are noted to be aligned to prepare students for industry certifications through CompTIA and Linux Professional Institute/Linux essentials.

The William Woods University Cybersecurity program's unique features include an experiential learning component (students either complete an internship or independent study project during their time in the program) and the IBM Cybersecurity Analyst Professional Certificate offered through Coursera that has been embedded into classes throughout the program.

References

CyberSecurityDegree.com. (2022, January 25). *Interview with Angela Holden, DM, PMP about the B.S. in Cybersecurity and M.S. in cybersecurity management at Lindenwood University*. CyberSecurityDegree.com. https://www.cybersecuritydegree.com/school-interviews/angela-holden-lindenwood-university#:~:text=something%20disastrous%20happening.-,It%20is%20the%20principle%20of%20%E2%80%9CProtect%2C%20Detect%2C%20Respond%E2%80%9D,right%20before%20the%20pandemic%20started.

Lindenwood University Online. (2025, May 21). *Online cybersecurity bachelor's degree: Lindenwood Online*. Lindenwood University Online. https://online.lindenwood.edu/programs/bachelors-cybersecurity/

Maryville University. (2023, November 8). *Online bachelor's in cybersecurity curriculum*. Maryville University Online. https://online.maryville.edu/online-bachelors-degrees/cyber-security/curriculum/

Maryville University. (2024, February 28). *New federal designation for Cybersecurity Program*. MPress. https://www.maryville.edu/mpress/new-federal-designation-for-cybersecurity-program/

Degree Completion by Institution - 2023

Compare degree completions and associated market data among your comparison group. Tuition & Fees data provided by IPEDS.

INSTITUTION	DEGREE COMPLETIONS	GROWTH % YOY	MARKET SHARE	UNDERGRADUATE TUITION & FEES	GRADUATE TUITION & FEES
Maryville University of Saint Louis (Saint Louis, MO)	155	**+ 17.42%**	88.1%	$27,166	$15,766
Bachelor's Degree	78	**+ 5.41%**	44.3%	-	-
Master's Degree	77	**+ 32.76%**	43.8%	-	-
Doctor's Degree	No Data	No Data	No Data	-	-

Associate's degree	No Data	No Data	No Data	-	-
Lindenwood University (Saint Charles, MO)	18	**- 43.75%**	10.2%	$21,100	$8,550
Bachelor's Degree	18	**- 25.00%**	10.2%	-	-
Master's Degree	No Data	No Data	No Data	-	-
Doctor's Degree	No Data	No Data	No Data	-	-
Associate's degree	No Data	No Data	No Data	-	-
William Woods University (Fulton, MO)	3	**+ 50.00%**	1.7%	$28,860	$13,800
Bachelor's Degree	3	**+ 50.00%**	1.7%	-	-
Master's Degree	No Data	No Data	No Data	-	-
Doctor's Degree	No Data	No Data	No Data	-	-
Associate's degree	No Data	No Data	No Data	-	-

Source: Lightcast

Senior Exit Surveys

1. What were some positive and negative feedback received from students as they complete their degrees?
2. Highlight any trends or insights that came from exit surveys over the course of the cycle.

Narrative:

No Senior Exit Surveys have been collected as of this review cycle.

Graduate/Alumni Feedback on the Program

1. What were some positive and negative feedback received from alumni?
2. Highlight any trends or insights that came from alumni feedback over the course of the cycle.

Narrative:

No Graduate/Alumni Feedback Surveys have been collected as of this review cycle.

Recommendations from Previous Program Reviews

1. Summarize recommendations from previous PRs, describe how those recommendations were applied throughout this cycle.

Narrative:

Notes from prior program reviews have included the following:

"The program has an outstanding adjunct faculty in the on-line program. The program now has a full time
professor on campus and is now building it's on campus program. Also, the program is being structured so that WWU students can take Cyber courses as electives and select the program as a minor. There are all good points moving forward."

The primary weakness previously noted was that the Cybersecurity program still has a limited presence on campus.

Recommendations were made for the program to focus on the following:

"Continue building the on-campus program and try and find some adjunct faculty to teach on campus classes to augment the full-time staff. Build a relationship with the US Cyber Range to offer hands-on Cybersecurity Labs to enhance the student learning."

Based on these notes, the Cybersecurity program has been able to address many of these points throughout the most recent review cycle. The Cybersecurity program has developed a stronger presence on-campus during the second half of this review cycle with larger enrollment on-campus in the major, adding the Cybersecurity minor to the academic catalog, adding two Cybersecurity courses to the general education offerings, providing field trip opportunities to Cybersecurity majors, and hosting numerous LEAD events (many of which were student-led) on campus.

Over the review cycle, the US Cyber Range and Enterprise KC/Heartland Cyber Range have both been explored as potential options to implement additional lab and experiential learning opportunities within the Cybersecurity program. At this time, additional online adjunct faculty are being considered for the increased enrollment in that modality of the program.

Industry Relevance and Employment

1. How do your student learning outcomes align with industry needs?

Narrative:

The following are the program objectives/student learning outcomes for the Cybersecurity Program:

P1. Discuss the impact of cybersecurity on society and organizations.
P2. Develop presentations and documentation to communicate technical content.
P3. Describe the process of designing a computer system.
P4. Design and implement cybersecurity solutions based on a set of requirements.
P5. Identify and compare computer networks and architectures.
P6. Communicate computer security principles and their application.

The student learning outcomes align with industry needs by addressing technical skills as well as soft skills that are necessary for success within the Cybersecurity/Information Security workforce. With Program Objective 1, students are able to demonstrate understanding of the role of cybersecurity within their own position or team as well as how cybersecurity affects other units or teams within their organization. Students are challenged to consider financial, technical, reputational, and operational impacts of cybersecurity (or the effects of its absence) to get a more holistic view of how cybersecurity principles affect organizations and society overall including systems, people, and critical infrastructures.

Program Objective 2 and Program Objective 6 require students to be able to articulate their ideas and share them with audiences in various contexts from end users to leadership teams, to other cybersecurity professionals. Students become experienced in communicating their ideas and cybersecurity principles in written and verbal formats which are crucial skills for working within teams and effectively collaborating with others.

Program Objectives 3, 4, and 5 reinforce the technical skills being learned in each of the courses and are broad enough to include new and emerging technologies as they become embedded into systems and organizations. Students are able to describe how computers and information systems function, note where security gaps occur within these systems, identify and apply best security controls, and consider how systems and the security controls chosen to interact with each other to best support business needs.

Employment Outlook

1. Describe employment outlook for the degree.
2. What types of employment would constitute working "in the field?"
3. Are there changes to program offerings and activities that would improve the employment outlook for graduates?

Narrative:

Cybersecurity jobs consist of a broad variety of job titles as well as the types of work completed within these roles. Employment within the Cybersecurity field can include roles

such as Cybersecurity/Information Security Analyst, Security Operations Center (SOC) Analyst, Penetration Tester, Cybersecurity Engineer, Network/System Administrators, Database Administrator, and Incident Responder. Roles can also specialize in areas such as Cloud Security; Governance, Risk, and Compliance (GRC); Auditing, or leadership roles such as Chief Information Security Officer (CISO).

The job openings for roles of Computer and Information Systems Managers, Database Administrators, Health Information Technologists and Medical Registrars, Information Security Analysts, and Network and Computer Systems Administrators are all projected to grow anywhere from 0.96% to over 13% between 2024 to 2029 (Lightcast Labor Market Overview).

Regional job trends demonstrate growth for both regional and national jobs available over the past twenty years with only a slight decline regionally in 2024 that is projected to show growth again leading into 2029 (Lightcast Regional Job Trends).

Compensation for median and high earners in the Cybersecurity field exceeds $100,000 both regionally and nationally with low earners still earning nearly $60,000 regionally and $72,000 nationally (Lightcast Regional Compensation Trends).

The core courses have stayed the same for the Cybersecurity program, but the curriculum continues to be adapted to meet the needs of the evolving job market. Program offerings and activities that have been implemented to improve employment outlook for graduate include a field to the STL CyberCon that features a Cybersecurity-focused job fair, embedding the IBM Cybersecurity Analyst Professional Certificate offered through Coursera into courses, and inviting representatives from the Information Technology Services Division (ITSD) for the State of Missouri to the on-campus career fair to share employment opportunities with students.

Regional Job Trends

View job trends for your region as compared to national trends for the past two decades and the 5-year projection.

YEAR	REGIONAL JOBS	REGIONAL PERCENT CHANGE	NATIONAL JOBS	NATIONAL PERCENT CHANGE
2004	36,187	-	623,595	-
2009	43,391	**+ 19.91%**	743,799	**+ 19.28%**
2014	48,015	**+ 10.66%**	856,537	**+ 15.16%**
2019	49,533	**+ 3.16%**	1,018,098	**+ 18.86%**

2024	49,345	**- 0.38%**	1,238,135	**+ 21.61%**
5 Year Projected (2029)	52,548	**+ 6.49%**	1,366,296	**+ 10.35%**

Source: Lightcast

Regional Compensation Trends

Compare compensation data for target occupations in your region to national and cost of living adjusted compensation trends in 2024.

EARNERS	REGIONAL COMPENSATION	NATIONAL COMPENSATION	COST OF LIVING ADJUSTED COMPENSATION
Lowest Earners	$59,563	$72,265	$63,057
Median Earners	$108,074	$135,701	$114,414
Highest Earners	$184,397	$236,189	$195,214

Source: Lightcast

Labor Market Overview

View the key labor market data for your region compared to national data.

49,345	6.5%	$44.87	3,914
Jobs in 2024 **99% Below National Average**	Change from 2024-2029 **+10.4% National Change**	Median Earnings per Hour **$50.30/hr. National Median**	Annual Openings **134% Below National Average**

OCCUPATION	2024 JOBS	GROWTH (2024-2029)	MEDIAN EARNINGS	ANNUAL OPENINGS

Computer and Information Systems Managers	22,299	**+ 8.31%**	$68.89/hr.	1,940
Database Administrators	3,106	**+ 1.93%**	$44.87/hr.	210
Health Information Technologists and Medical Registrars	2,657	**+ 7.72%**	$28.08/hr.	221
Information Security Analysts	6,857	**+ 13.81%**	$49.05/hr.	636
Network and Computer Systems Administrators	14,426	**+ 0.96%**	$39.87/hr.	907

Source: Lightcast

External Review

Executive Summary

General observations and comments are provided as to how the program aligns with and supports the University mission and curriculum, the quality of student learning and the achievement of student learning outcomes, the qualifications and achievements of faculty, the student experience, the state of facilities, the value of online resources and supports (if relevant), on-campus resources, financial resources, and how the program is responding to trends within the larger perspective of the program field.

Narrative:

- The cybersecurity degree program is an excellent degree to prepare students for valuable jobs and careers. I've seen estimates of at least 750,000 unfilled cybersecurity jobs in the U.S.
- The program has done an excellent job implementing the online degree and course program to respond to student needs for off-campus and non-traditional learning. Offering online courses and an online degree are essential to current and future recruitment.
- William Woods' cybersecurity degree program does a good job balancing the educational needs for both technology skills and business skills.
- Having three courses from the Criminal Justice degree program is an excellent inclusion.
- The diverse learning opportunities with the LEAD program, STL CyberCon, and internships is excellent.
- Instructors all have excellent credentials and experience.
- The online courses' use of varied resources including Coursera brings detailed and established resources into the student experience.

- Students I spoke with felt online learning was valuable and worked well for most courses. Social Engineering was cited as one of the best courses. Difficulty and effectiveness depended on the subject, instructor and resources (like textbooks). They did state "a few" instructors do not provide feedback to assignments and did not seem to be engaged.
- Students I spoke with stated campus resources were "really good." The new lab was cited as a big plus, and dual monitors were helpful. All complimented Nina specifically for the quality of the lab and resources.
- Students did state it would be nice to have a room and network solely dedicated to them with more hands-on equipment. This would be a "secure" location and network just for them to simulate security problems and fixes.
- Career counseling and placement:
    - Students commented that, as they approached graduation, they did not have any idea where to start looking for a job, which job titles or positions are best for new graduates, and which to explore for good alignment with their interests.
    - Students commented that Nina was a great resource and emailed internship opportunities.
    - Students commented that besides Nina, resources on campus were almost non-existent. The career counseling office was "not helpful."
- Students indicated the university, and instructors do a good job explaining clear guidelines for AI use in courses including when it is allowed/encouraged and when it is not allowed. They also indicate the university is open to discussing changes in policy and evaluation of use cases. However, they have concerns as they believe some students are still using it outside of allowed use cases. This is a very challenging topic.
- The university has been responsive to changes in student degree program needs with new sports management and cybersecurity degrees.
- The university is investing in the campus with a new dorm and the new computer lab.

Commentary

Reviewers provide comments about the program strengths and challenges.

Narrative:

Strengths:

- The degree is in high demand with excellent hiring prospects for graduates.
- WWU's program addresses a growing demand for online, asynchronous degree programs.
- WWU offers a strong combination of well-qualified instructors.
- The degree program offers diverse learning opportunities with the LEAD program, STL CyberCon, and internships.
- The new on campus lab.
- The degree's inclusion of courses in Criminal Justice and Business, all critical in cybersecurity.
- The on-ground faculty person was repeatedly cited by students as a tremendous professor and resource to them.
- Students find the university's process to address AI use in education is effective and the university listens to student input.

Challenges:

- Comments from students indicate concerns with having just one on-ground professor for coverage of all student needs and a growing program even though that person has always been available for their needs.
- AI use in education is an incredibly challenging topic and difficult to evaluate and balance in learning environments.
- Providing students with sufficient resources for career planning and job placement after graduation.
- Declining university enrollment nationwide.
- Nationwide trend in students transferring universities.

Recommendations

Comments provide future direction for the faculty to use to improve student learning. Evaluative feedback is offered, as well as suggestions to improve any aspect of the program. Recommendations that require no new resource as well as those that do are welcome, alongside identifying areas for program development based on market/industry demands not yet identified by the university or program faculty. The report may include recommendations that have been shown to be effective elsewhere.

Narrative:

I see many strengths in the program both from my review and the student interview comments. The following are just suggestions for improvement of a valuable and successful degree program.

1. Include at least two Generative AI courses in the degree program or significantly integrate in all relevant existing courses.
    1. GenAI is the most transformational technology in at least the last 20 years and is being incorporated today in cybersecurity systems like SIEM, patching, and code generation for scripting. Soon it will automate incident and vulnerability response among others.
    2. The university must prepare students for this technology that will be ever present when they graduate.
    3. The university can really stand out and be a leader by offering courses that will prepare students for what may be a competitive job market for new graduates. This would be easier to stand out if specific courses were offered.
2. Improve career counseling and preparation.
    1. Students all shared this as a weakness for the program.
    2. Ideas include bringing in cybersecurity professionals for a “career day” or as guest speakers.
    3. Help students understand the cybersecurity job titles, responsibilities, and hiring prospects.
3. My interpretation of numerous comments from on-campus students is Nina is essentially most of the program at this point in time and it continues to grow. Students commented that she does a “tremendous job” and is always available for whatever they need. Other comments from students expressed concern for her workload, especially if the program continues to grow.

    1. Consideration should be given to bringing in a second faculty member especially as the program grows. This will give Nina and students more resources. This will also give the university a second person on-campus for a growing program, and better continuity for the program with two full-time faculty.
    2. This may also help coverage of Generative AI in the program.
4. Work with the State of Missouri - Department of Public Safety to partner on their cybersecurity operations. This could be for speakers, on-site learning, internships, and other partnerships. DPS is a partner with CISA and coordinates all cybersecurity operations within MO state government just 25 miles away.
5. Facilitate connecting students with more internship opportunities. A second faculty member could also help with this.

Program Response to External Review

Program Response

After the External Report is submitted, the Program faculty will respond to any comments where the reviewer has noted need of improvement or where additional explanation is needed. The faculty response will also include a response to the recommendations of the reviewer and their action plan to move forward with recommendations, or what is needed for the program to move forward with a recommendation. This response is added to the report and submitted to Academic Council for final review.

Narrative:

The William Woods Cybersecurity Program has taken steps to address some of the areas noted in the External Report already as well as other areas that can benefit from improvements/innovations. The Cybersecurity Program plans to continue recognizing Cybersecurity Awareness Month in October with LEAD Events as well as hosting additional related LEAD Events throughout the academic year. The CSS 490 - Cybersecurity Capstone class will once again participate in the Symposium for Scholarship, Research, and Creativity (along with alternating courses in the program based on course rotations) to give students experience presenting to a variety of audiences. The Cybersecurity Program has begun working with the University Information Technology (UIT) department as of Summer 2025 to establish a Virtual Local Area Network (VLAN) to provide network segmentation for Cybersecurity students to be able to conduct more robust projects/labs/exercises in a secure environment.

In the past, Student Performance Days hosted in February of each year have included a component where all on-ground Cybersecurity majors make updates to their LinkedIn profiles created within the CSS 210 - Introduction to Cybersecurity-Q course. Other activities in past years have included hosting virtual panels of industry professionals for Q&A or representatives of graduate level Cybersecurity programs to share with students about Cybersecurity-specific opportunities following graduation.

Next steps to further address some of the recommendations made in the External Report include looking at adding a potential second field trip opportunity in the Spring (the STL CyberCon is hosted in October/November each year), to give students additional industry

exposure. Based on the feedback provided by students and within the External Report, career planning and job placement resources will become a major focus going into this academic year including reaching out to adjunct instructors about resources they may be able to share, reinforcing relationships with local organizations like the Information Technology Services Division (ITSD) for the State of Missouri, and inviting recent alumni back to campus to share about their internship/early career experiences. Additional work study positions within the Cybersecurity Department are also being offered/filled this academic year to give students more professional experience/continue to develop additional programming within the department.

Faculty workload is regularly reviewed with respect to the number of incoming Cybersecurity majors and courses that are also required for Computer Information Systems majors and/or that are part of other academic programs. An additional online adjunct was hired during the last academic year to facilitate courses offered within both the Cybersecurity (CSS) and Computer Information Systems (CIS) programs.

The IBM Cybersecurity Analyst Professional Certificate that is offered through Coursera and is built into the WWU Cybersecurity program has recently been updated (as of Summer 2025) to include some content/modules related to AI. As curriculum is regularly reviewed, the program can also look towards integrating more Artificial Intelligence (and other emerging technology) content into courses. The newly implemented Computer Information Systems major includes a course (CIS 311 - Artificial Intelligence and Impact) that can also be reviewed for potential future inclusion within the major.

The WWU Cybersecurity program will also look into working with the State of Missouri - Department of Public Safety to partner on their cybersecurity operations. As noted in the External report, "This could be for speakers, on-site learning, internships, and other partnerships. DPS is a partner with CISA and coordinates all cybersecurity operations within MO state government just 25 miles away."

Academic Council Review

Academic Council Response

Academic Council will review the report in its entirety and come together to discuss any remaining questions or concerns. The council will highlight noted areas of improvement for program focus. Issues of resources are discussed if additional resources are needed to implement improvements noted by the Reviewer, the faculty or Academic Council.

Narrative:

AC Review: Cybersecurity

Strengths:

- It appears that adjunct qualifications are more than adequate (lots of professional, academic and military experience related to the field). Online programming in the field seems to continue to grow.

- The report details the program contribution to student culture on campus, through conference attendance, LEAD events, etc.
- Well-developed response to how program builds on GE areas.
- "Positive projection for job employment in the field. Field is constantly changing - need for ongoing PD for instructors and program managers. "
- The entire report was very well-written and clear and included all of the evidence needed.

Challenges:

- The program only has one on ground advisor/faculty member for the number of students in the program.
- It was challenging in the report to know if the data was referencing online or on-ground issues. This led to weaknesses when talking about rotation and assessment (p 8).
- The discussion regarding the rationale for alignment to GE could be strengthened.
- The field is relatively new but also certification driven in a way that advanced degrees are not the standard for skills qualification. This adds to the difficulty of ensuring that the program is meeting accreditation standards.
- The rationale for why Criminal Justice courses play a role in the program objectives is not clearly defined.
- Display of data for the snapshot of assessment should show the data instead of representing the data in only a narrative way.

Action Items:

- AI content covered in the curriculum
- Proposal for an additional faculty member and how the specializations of faculty would diversify the curriculum in the program
- Identify opportunities for career counseling for students in the program so that they are better informed as to job prospects upon graduation – (Advising tool kit)
- Look at how to build in redundancies so that all of the productivity does not fall on one faculty so that the program is more sustainable.
- The program could review the offerings online and on ground and evaluate if more courses could be offered on ground instead of so many online only (student retention and engagement for on campus students)
- The program should investigate the idea of an isolated server/network so that students could run simulations and practice – this would be a strong addition to the curriculum.
- Implementation of a pre/post evaluation for majors is generally a strong assessment tool that helps to fill in gaps when courses are inconsistent in offering as well as faculty/curriculum. the program should look at standardized options or work out a performance task or evaluation that is internal for students to take.

-