DEPARTMENT OF HIGHER EDUCATION & WORKFORCE DEVELOPMENT

New Program Report

Date Submitted:
01/17/2024

Institution
Missouri Valley College

Site Information

Implementation Date:
8/19/2024 12:00:00 AM

Added Site(s):

Selected Site(s):

Missouri Valley College, P.O. Box 1000, Marshall, MO, 65340

CIP Information

CIP Code:
111003

CIP Description:
A program that prepares individuals to assess the security needs of computer and network systems, recommend safeguard solutions, and manage the implementation and maintenance of security devices, systems, and procedures. Includes instruction in computer architecture, programming, and systems analysis; networking; telecommunications; cryptography; security system design; applicable law and regulations; risk assessment and policy analysis; contingency planning; user access issues; investigation techniques; and troubleshooting.

CIP Program Title:
Computer and Information Systems Security/Information Assurance

Institution Program Title:
Cybersecurity

Degree Level/Type

Degree Level:
Bachelor's Degree

Degree Type:
Bachelor of Science

Options Added:

Collaborative Program**:**
Y

Mode of Delivery

Current Mode of Delivery

Hybrid

Online

Student Preparation

DEPARTMENT OF HIGHER EDUCATION & WORKFORCE DEVELOPMENT

New Program Report

Special Admissions Procedure or Student Qualifications required:
N/A

Specific Population Characteristics to be served:
N/A

Faculty Characteristics

Special Requirements for Assignment of Teaching for this Degree/Certificate:
All MVC faculty teaching courses in this program possess the minimum qualifications set forth in the MVC Faculty Minimum Qualifications & Equivalent Experience Policy.

Rize instructors undergo two rounds of vetting: first by the Rize Academic team (including the Chief Academic Officer) and then by the Teaching Institution (TI) of record, which is Adrian College for Cybersecurity). The Rize Academic team first sources the instructors and requires minimum qualifications of 1) at least a Master's degree in a relevant field and/or 2) 10+ years of industry experience. Rize also prioritizes experience with online learning as well as experience teaching to a variety of levels in the classroom.

Candidates who pass the Rize interview process will then move on to the Teaching Institution vetting process. Rize asks the TI to vet each instructor as if they were hiring an adjunct faculty member. Once a candidate passes the TI interview process, they are onboarded and hired by that TI as an adjunct faculty member. All institutions, both home and teaching, have access to instructor CVs and credentials at all times.

Estimate Percentage of Credit Hours that will be assigned to full time faculty:
Full time faculty at MVC will teach 60-70% of the credit hours required in this program. MVC adjunct faculty will teach 10-20% of the required credit hours. Rize/LCMC instructors will teach 17.5% of the required credit hours.

Expectations for professional activities, special student contact, teaching/learning innovation:
Annual professional development initiative; weekly visible contact with students; weekly feedback in response to student work; collect and use student feedback for continuous professional improvement.

Student Enrollment Projections Year One-Five

Year 1	**Full Time:** 10	**Part Time:** 0	
Year 2	**Full Time:** 15	**Part Time:** 0	
Year 3	**Full Time:** 20	**Part Time:** 0	**Number of Graduates:** 5
Year 4	**Full Time:** 25	**Part Time:** 0	
Year 5	**Full Time:** 30	**Part Time:** 0	**Number of Graduates:** 16

Percentage Statement:
80.00

Program Accreditation

Institutional Plans for Accreditation:
The degree proposal will be sent for approval by the Higher Learning Commission upon approval from MDHE.

DEPARTMENT OF HIGHER EDUCATION & WORKFORCE DEVELOPMENT

New Program Report

Program Structure

Total Credits:
120

Residency Requirements:
N/A

General Education Total Credits:
42

Major Requirements Total Credits:
51

Course(s) Added

COURSE NUMBER	CREDITS	COURSE TITLE
BNSS 212	3	Principles of Management
PMM I	3	Introduction to Project Management
CYS III	3	Modern Cybersecurity
BNSS 412	3	Administrative Communications
CYS IV	3	Network & System Security
CYS V	3	Cyber Forensics
CYS II	3	Cybercrime & Governance
CYS VI	3	Capstone - Ethical Hacking
CPSC 170	3	Programming I
BNSS 422	3	Organizational Behavior
CPSC 110	3	Intro to Computer Information Systems
CPSC 320	3	Data Communications
CPSC 1XX	3	Introduction to Cybersecurity
PSYC 100	3	Principles of Psychology
Cloud 0	3	Google Cloud Computing Foundations
CPSC 4XX	3	Cybersecurity Internship
CPSC 120	3	Introduction to Programming

Free Elective Credits:
27

Internship or other Capstone Experience:
CYS VI 3 Capstone - Ethical Hacking: Students must complete a hands-on project where they are asked to ethically hack a real system.CPSC 4XX Cybersecurity Internship: Professional work experience (minimum 150 hours) in applied cybersecurity.

Assurances

DEPARTMENT OF HIGHER EDUCATION & WORKFORCE DEVELOPMENT

New Program Report

I certify that the program will not unnecessarily duplicate an existing program of another Missouri institution in accordance with 6 CSR 10-4.010, subsection (9)(C) Submission of Academic Information, Data and New Programs.

I certify that the program will build upon existing programs and faculty expertise.

I certify that the institution has conducted research on the feasibility of the proposal and it is likely the program will be successful. Institutions' decision to implement a program shall be based upon demand and/or need for the program in terms of meeting present and future needs of the locale, state, and nation based upon societal needs, and/or student needs.

Contact Information

First and Last Name: Joseph Alsobrook

Email: alsobrookj@moval.edu

Phone: 660-831-4021

January 2024

Proposal
Through a partnership with RIZE Education and LCMC, offer a **BA/BS in Cybersecurity** degree through an online or hybrid format (i.e., some courses will be available to take on-campus). RIZE/LCMC courses, however, will only be available online.

School
Business and Technology

Program
BA/BS in Cybersecurity
CIP: 11.1003 Computer and Information Systems Security/Auditing/Information Assurance

Program Contact
tAno Mateu, MVC Chief Information Security Officer

Why Cybersecurity?
It has become incredibly cheap to automate constant digital attacks against any individual, Fortune 500 corporation, or government system. As a result, we now live in a world where we can assume that everyone is constantly at risk of attack from advanced cyber threats. This new paradigm has led to a boom in cybersecurity careers. According to LightCast, cybersecurity professionals earn a median salary of $102,527, with entry-level positions starting at $68k. Furthermore, there is virtually zero-percent unemployment within the field of cybersecurity, and approximately 460,000 unfilled positions in the US alone. According to Cyber Seek, the state of Missouri is experiencing a deficit of cybersecurity professionals at 15K+ job openings, and about 2.5K of those openings request a Certified Information Systems Security Professional (CISSP) certificate.

About the Program
Within this program, students will assess modern cybersecurity challenges that threaten our privacy, security, and safety, and gain both the knowledge and hands-on technical skills to protect digital assets from cybercriminals who leverage sophisticated social and cyber tactics to facilitate attacks.

Students who complete this curriculum will not only be prepared for a career as a cybersecurity professional, but they will also be well-positioned to obtain a number of certifications that will increase their employability, including Certified Ethical Hacker, Certified Information Systems Security Professional, and Certified Forensic Examiner.

Credit Hour Breakdown

General Education Core (including College Algebra)	42

Major	51
Electives/Minor (12 hours 300-400 level)	27
Total	120

Student Learning Objectives

- Successfully sit for the Certified Computer Forensics Examiner (CCFE) exam with minimal additional preparation
    - Cybercrime and Governance, Cyber Forensics
- Understand and apply all concepts tested by the Certified Ethical Hacker (CEH) exam
    - Capstone - Ethical Hacking
- Understand and apply all concepts tested by the Certified Information Systems Security Professional (CISSP) exam
    - Introduction to Cybersecurity, Network and System Security, Capstone - Ethical Hacking
- Understand the range of cyber threats present in modern society
    - All cybersecurity courses
- Secure vulnerable technical resources against a range of cyber threats and attacks
    - Introduction to Cybersecurity, Modern Cybersecurity, Network and System Security, Capstone - Ethical Hacking
- Identify and test vulnerabilities in a system
    - Introduction to Cybersecurity, Network and System Security, Capstone - Ethical Hacking
- Protect both individual and organizational online privacy
    - Introduction to Cybersecurity, Modern Cybersecurity, Network and System Security, Capstone - Ethical Hacking
- Identify threat actors
    - Cybercrime and Governance, Cyber Forensics
- Conduct a Cyber Forensic investigation of a security breach
    - Cybercrime and Governance, Cyber Forensics

Major Courses

Number	Name (Weeks)	Prerequisites	Credit Hours	300+ Credit Hours	Rotation
CPSC 110	Intro to Computer Information Systems (16)		3		Fall Online - Fall
CPSC 1XX	Introduction to Cybersecurity (8)		3		Online - Fall, Spring
*PMM I (100)	Introduction to Project Management (14)		3		Online - Fall, Spring

PSYC 100	Principles of Psychology (8)		3		Fall Spring Online - Fall Online - Spring Online - Summer
CPSC 120	Introduction to Programming (16)	MATH 165+	3		Fall Online - Fall
CPSC 170	Programming I (16)	CPSC 120, MATH 165	3		Spring Online - Spring
BNSS 212	Principles of Management (8)	ENGL 160	3		Fall Spring Online - Fall
*CYS II (200)	Cybercrime & Governance (14)	CPSC 1XX	3		Online - Fall, Spring
*CYS III (200)	Modern Cybersecurity (14)		3		Online - Fall, Spring
*Cloud 0 (200)	Google Cloud Computing Foundations (14)		3		Online - Fall, Spring
*CYS IV (300)	Network & System Security (14)		3	3	Online - Fall, Spring
ENGL 327 -or- BNSS 412	Technical & Professional Writing (16) Administrative Communications (8)	ENGL 160 Sr. Standing	3	3	Spring odd years Online - Spring even years Fall Spring Online - Summer
*CYS V (300)	Cyber Forensics (14)	CYS I, CYS II	3	3	Online - Fall, Spring
CPSC 320	Data Communications (16)	CPSC 110 or 105, MATH 165+	3	3	Fall Online - Fall
BNSS 422	Organizational Behavior (8)	BNSS 212	3	3	Fall Online - Fall
*CYS VI (400)	Capstone - Ethical Hacking (14)	CYS IV	3	3	Online - Spring
CPSC 4XX	Cybersecurity Internship (16)	Junior or Senior Standing and Permission of Instructor, School Dean, and VPAA.	3	3	Arranged
		TOTALS	51	24	

* RIZE/LCMC Courses

RIZE Courses

PMM I Introduction to Project Management (3)

According to a recent study of human resource managers, effective project management is one of the most coveted skills for new hires in the modern economy. This course will introduce you to the power of effective project management through two primary frameworks: waterfall and agile. You will also learn vital project-management concepts that can be applied to a wide range of industries and occupations. This online class has optional live sessions. Prerequisite: Junior or Senior Standing and Permission of Instructor, School Dean, and VPAA.

CLOUD 0 Google Cloud Computing Foundations (3)

This course will introduce you to the fundamentals of Cloud Computing, Infrastructure and Networking, and will explore how the cloud is used in a range of situations, including IT, App Development and Machine Learning. By the end of the course you will know what the cloud is, and how to use it effectively. This course uses the Google Cloud Platform (GCP) and was built in concert with the Google Cloud Learning Services team. This online class has optional live sessions.

CYS II Cybercrime & Governance (3)

Cybercrime is one of the biggest threats companies face on a daily basis, and they are constantly looking for new hires to help protect them. In this course, you will get a firsthand look at the methods used to commit cybercrimes. You will also learn how governments detect, investigate, and stop these crimes, and become familiar with the laws and policies in place to deter cybercriminals. This online class has optional live sessions.

CYS III Modern Cybersecurity (3)

Just as technology is constantly evolving, so too must cybersecurity to keep pace with changing trends. In this class, you will learn about the changing landscape of cybersecurity, emerging mobile technologies that are likely to be targeted, and new forms of cyber-attacks being launched. By the end of the course, you will be able to implement the most up-to-date practices in cybersecurity in order to protect against attacks. This online class has optional live sessions.

CYS IV Network & System Security (3)

Modern organizations know that even the strongest systems can be vulnerable to cyber-attacks. As a result, jobs in cybersecurity are rapidly expanding as companies look to secure their digital assets. This course will teach you how to secure those assets by identifying and fixing potential security vulnerabilities. By the end of the course, you will be able to identify and remedy common network and systems vulnerabilities. This online class has optional live sessions.

CYS V Cyber Forensics (3)

When cybercrimes do happen, you need to know how to respond. This course examines the tools and techniques used to perform cyber forensics and conduct investigations into cybercrimes. By the end of the course, you'll be able to gather and analyze important digital evidence and gain skills in analyzing cybercrime that are in demand from companies across the country. This online class has optional live sessions.

CYS VI Capstone - Ethical Hacking (3)
To stop a hacker, you need to be able to think like a hacker. In this course, you will learn hands-on techniques for attacking and penetrating networks and systems. You will be prepped with tools to launch these offensive tactics, and then complete a hands-on project where they are asked to ethically hack a real system. This online class has optional live sessions.

Note: Each RIZE course will be given a MVC course number.

New MVC Courses (tAno Mateu, Instructor)

CPSC 1XX Introduction to Cybersecurity (3)
In today's world, no one is safe from cyber-attacks, but everyone can be prepared. This course will teach you how malicious actors use social skills and technology to facilitate cyber attacks and provide you with the tools and information you need to defend against those attacks. Whether you pursue one of the many available jobs in cybersecurity or just want to secure your own privacy, you'll learn how to make the Internet safer. This online class has optional live sessions.

Student Learning Objectives

- Identify emerging cybersecurity risks (threats, vulnerabilities) to online privacy and security.
- Use encryption to keep your most personal information private.
- Protect an individual's online privacy and security via hands-on experience with a range of open-source cybersecurity tools.
- Analyze a multi-faceted cyber attack from the different phases of a successful hack.
- Detect cybersecurity events that pose a threat to online privacy and security.
- Take appropriate actions to respond to a cybersecurity event and recover any capabilities that were impaired due to the event.
- Execute a risk assessment to determine where you may be most susceptible and vulnerable to a cyber attack.
- Prepare a comprehensive risk management plan that assesses the risk of online privacy and security and recommends mitigations.
- Communicate cybersecurity vulnerabilities and best practices to others.
- Implement defense-in-depth cyber tools and practical countermeasures on your home network.

CPSC 4XX Cybersecurity Internship (3)
Professional work experience in applied cybersecurity. This internship is contracted by the student, on-site supervisor, faculty supervisor, and school dean.

RIZE Guaranteed Enrollment Dates

Cybersecurity

Cybersecurity Overview

Why This Matters

It has become incredibly cheap to automate constant digital attacks against any individual, Fortune 500 corporation, or government system. As a result, we now live in a world where we can assume that everyone is constantly at risk of attack from advanced cyber threats.

This new paradigm has led to a boom in cybersecurity careers. According to LightCast, cybersecurity professionals earn a median salary of $102,527, with entry-level positions starting at $68k. Furthermore, there is virtually **zero-percent unemployment** within the field of cybersecurity, and approximately **460,000 unfilled positions** in the US alone.

About

Our Cybersecurity major is designed with two goals in mind:

- To ensure that students stay one step ahead of evolving cyber threats.
- To provide students with fundamental IT skills.

While the first goal is primary and more foundational to a cybersecurity program, the importance of the second goal should not be disregarded for two major reasons. First, entry-level cybersecurity roles, as well as roles at smaller organizations, frequently blend elements of cybersecurity and IT work. Second, the cybersecurity function of an organization is inextricably linked with IT since both networks and team members present opportunities to bad actors. To that end, students who complete the recommended IT focus area will not only be prepared for numerous cybersecurity certifications; they will also be prepared for the CompTIA A+ exam.

Within this program, students will assess modern cybersecurity challenges that threaten our privacy, security, and safety, and gain both the knowledge and hands-on technical skills to protect digital assets from cyber criminals who leverage sophisticated social and cyber tactics to facilitate attacks.

Furthermore, as the cyber attack surface continues to expand via the proliferation of Internet of Things (IoT) devices, it is increasingly vital that students learn how to "harden" networks, systems, and endpoint devices against cyber attacks, topics which are covered in the course *Modern Cybersecurity*.

It is, however, impossible to create a perfectly secure system, so students will also learn how to perform cyber forensics to investigate, collect, and preserve digital evidence associated with a breach.

Finally, students will learn how to think like a "hacker" and use industry standard tools to find weaknesses in systems.

Students who complete this curriculum will not only be prepared for a career as a cybersecurity professional, they will also be well positioned to obtain a number of certifications which will increase their employability later in their career, including Certified Ethical Hacker, Certified Information Systems Security Professional, and Certified Forensic Examiner. Please note these certifications may require additional work experience and exam preparation!

Subject Matter Experts

Randy Rovesti - Randy is a professor of IT and Cybersecurity at Penn State, as well as an Engineering Manager at the Naval Nuclear Laboratory, where he focuses on both physical and cyber security systems. His expertise on both the academic and professional side of cybersecurity made him uniquely qualified to be the primary designer of the Cybersecurity program, as he possesses both a strong theoretical foundation, and the day-to-day experience of putting that experience into practice. Randy holds a Masters in IT from Carnegie Mellon University.

Dr. Charles Severance, *University of Michigan* - Dr. Charles Severance holds a PhD in Computer Science from Michigan State University. He is the former Executive Director of the Sakai Foundation, and one of the world's leading online CS educators. His contributions and curriculum form the basis of our programming curriculum

Professional Advisors

Alexey Malashkevich - Alexey is a highly respected engineer and engineering manager with strong experience in building cloud-based financial technology systems. His skill in building engineering teams gives him particular insight into the skills most valuable in today's technology workforce. Furthermore, his experience in cloud-based FinTech provides him with tremendous experience in understanding the cybersecurity needs of organizations which face particularly heavy attack. Alexey is the former CEO of Agile Code - a software development firm - and has 20 years of experience bringing software products to market.

In addition to Alexey, we consulted with two Cybersecurity experts who asked not to be named here due to the highly sensitive and public nature of their roles.

Certifications

Cybersecurity Curriculum Certifications

Program Requirements (36+ Hours)

Recommended CIP Code: 11.1003

Cybersecurity Courses - 18 Hours

CYS I - Introduction to Cybersecurity

CYS II - Cybercrime and Governance

CYS III - Modern Cybersecurity

CYS IV - Network and System Security

- *Please Note: Students who complete the IT Focus Area may take ITM V - Information Security and Data Protection **in lieu of** CYS IV.*

CYS V - Cyber Forensics

CYS VI - Capstone - Ethical Hacking

Home Institution Recommendations - 18 hours

- Technical Writing
- Project Management
- Principles of Management
- General Psychology
- Organizational Behavior
- Management Information Systems

IT Focus Area (Recommended) - 12-15 Hours

ITM I - Introduction to Information Technology Systems

ITM II - Networking Technologies and Telecommunications

Cloud 0 - Google Cloud Computing Foundations

- Introductory Programming Sequence

Other Links

❓ Cybersecurity Program FAQs

🍎 Example Cybersecurity Instructors

CYS Four Year Plan.pdf 51.1KB

Learning Objectives and Assessment

Cybersecurity Advisor Guide