Cyber100

BRADLEY University

BRADLEY.EDU/CYBERSECURITY

Table of Contents

Cyber 100 Overview

Cyber 100 is an exclusive cybersecurity event designed to introduce high school students to the critical importance of cybersecurity in today's digital landscape. This day-long event provides students with hands-on experiences, insights from professionals, and an exciting competition to test their skills. Through engaging sessions, students will gain a deeper understanding of cybersecurity best practices, academic and career opportunities, and real-world applications of cybersecurity principles. Cyber 100 is open to high school juniors in the Peoria, Illinois metropolitan area who have been nominated by a teacher, counselor, or staff member at their school.

Best Practices for Security and Privacy

Academic & Career Opportunities

Cybersecurity Competitions

Social Engineering

Cyber 100 Organizers

PROGRAM CHAIRS

Dr. Jacob Young
Associate Professor
jayoung@bradley.edu

Angelica Fanti
Instructor in Residence
afanti@bradley.edu

SUPPORT STAFF

Elaina Wamhoff
ewamhoff@mail.bradley.edu

Maria Bezmenova
mbezmenova@mail.bradley.edu

From the Director

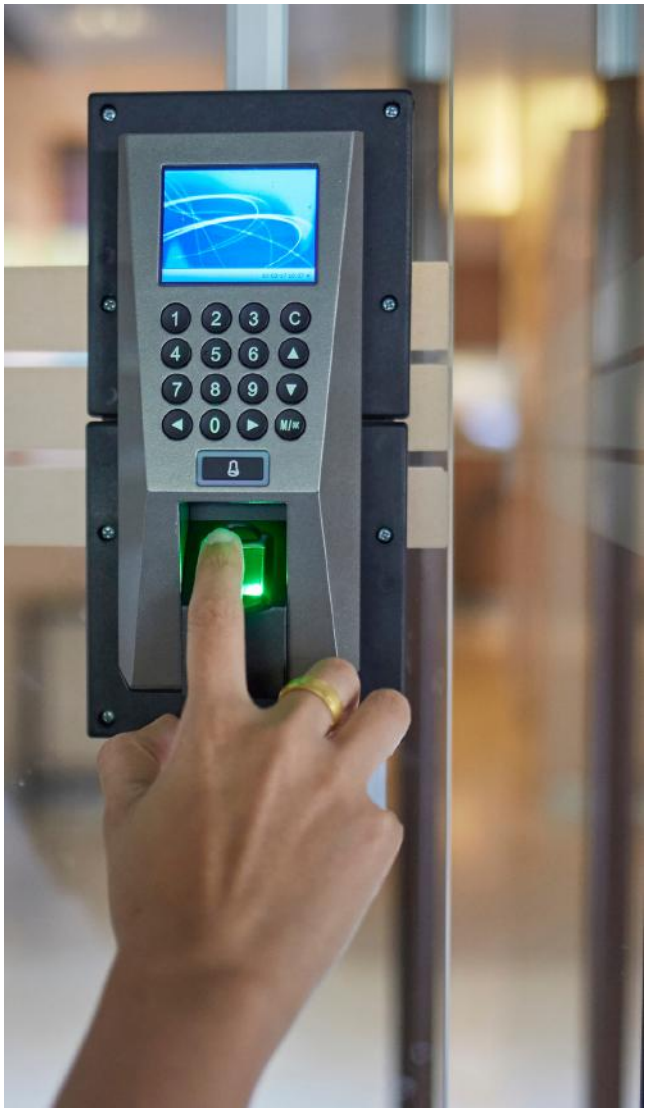
As the director of the Center for Cybersecurity at Bradley University, it is my pleasure to welcome you to Cyber 100! This special event is designed to ignite passions for one of the fastest-growing fields in the world. Cybersecurity is not just a career; it's a mission—a mission to protect the digital systems and networks that power everything from banking to healthcare to national security. Our goal is to expose you to the importance and excitement of cybersecurity while equipping you with the foundational knowledge to improve your own cybersecurity posture, and possibly shape your future career!

The need for skilled cybersecurity professionals has never been greater. Every day, cyber threats become more sophisticated, targeting individuals, businesses, and even governments. But with those challenges come incredible opportunities. In fact, the U.S. Bureau of Labor Statistics projects that the demand for information security analysts will grow by 35% in the next decade—far faster than the average for all occupations.

Through this program, you'll learn about risks we face in today's digital landscape and how cybersecurity professionals mitigate them. You'll engage in hands-on activities, hear from experts, and most importantly, discover how you can protect yourself and become a part of this vital field. We're excited to see what you accomplish today and in the years ahead. Let's do our part in securing a safer digital world!

Best,

Dr. Jacob Young
Director, Center for Cybersecurity



Eligibility

Cyber 100 is open to high school juniors from the Peoria, Illinois metropolitan area who have been nominated by a teacher or counselor. Students should demonstrate an interest in technology, problem-solving, or cybersecurity and have the potential to benefit from an introduction to career pathways in this field.

To be eligible for the program, students must:

- Be in their junior year of high school
- Attend a school in the Peoria metropolitan area
- Be nominated by a school employee
- Exhibit an interest in technology
- Have enthusiasm for developing new skills

Each student must be accompanied by a teacher or counselor. This ensures that participants have a supportive adult from their school community to guide them throughout the day and help them take full advantage of the program.

Nomination Process

The nomination process for the Cyber 100 program is designed to ensure that the students who attend have both the interest and potential to thrive in a cybersecurity-focused career. Teachers, counselors, and staff members are encouraged to identify students who have demonstrated an interest in technology or problem-solving and who they believe would benefit from an immersive experience in cybersecurity.

To nominate a student:

- **Complete the Nomination Form:** Teachers or counselors must complete the official Cyber 100 program nomination form, which can be **accessed here**.
- **Include a Short Recommendation:** The nominator should explain why the student would be a good fit for the program. This can include examples of the student's interest in technology, ability to solve complex problems, or their potential for growth in the field of cybersecurity.
- **Submit by Deadline:** Nominations must be submitted by **February 28, 2025**. Late nominations may not be accepted, so it's important to submit the form and recommendation on time.

The Cyber 100 selection committee will notify selected participants and their nominators by **March 7, 2025**. Teachers or counselors are expected to attend the program with their nominated student(s), providing guidance and support throughout the day.

Cyber 100 Schedule

FRIDAY, MAY 2, 2025

1	8:30-9:00 AM	Registration
2	9:00-9:30 AM	Welcome
3	9:30-10:30 AM	Breakout Session 1
4	10:30-11:30 AM	Breakout Session 2
5	11:30-12:30 PM	Lunch Session
6	12:30-1:30 PM	Breakout Session 3
7	1:30-2:30 PM	Breakout Session 4
8	2:30-3:00 PM	Closing Ceremony

The schedule is tentative and subject to change.

Security and Privacy

Attendees will gain a comprehensive understanding of how the dynamic global landscape and advancements in contemporary technology influence personal security, privacy, and individual freedoms. They will gain valuable insights into key topics such as:

- threat modeling
- secure account management practices
- data collection techniques
- identifying vulnerabilities across digital and physical environments.

Additionally, students will learn to apply robust security measures and leverage privacy-enhancing technologies to mitigate risks and address a wide range of real-world scenarios effectively.

Social Engineering

Students will learn about the human aspect of cybersecurity, focusing on how cyber criminals manipulate individuals to gain access to sensitive information. They will study various techniques such as phishing, baiting, and tailgating, examining how attackers manipulate trust, fear, or urgency to achieve their goals. Through the analysis of real-world case studies and engagement in practical exercises, students will cultivate the skills necessary to identify and respond to social engineering tactics.

Social engineering interesting facts:

- **Phishing is the most common form:** Attackers often send deceptive emails, or other types of messages to trick people into sharing personal information.
- **Social engineering attacks are responsible for 93% successful data breaches:** social engineering exploits human psychology, making it easier for attackers to manipulate individuals into revealing sensitive information.
- **On average, social engineering attacks cost $130,000**: social engineering attacks can cost organizations around $130,000. These costs often include reputation damage, operational disruptions, financial losses, legal costs, etc.
- **45% of employees don't report suspicious messages out of fear of getting in trouble:** employees worry about appearing incompetent, feeling embarrassed about falling for a scam, or simply not understanding the severity of the threat.

Cybersecurity Competition

Cybersecurity competitions consist of fun and interactive games designed to help students practice and learn important skills like hacking and protecting systems, problem solving, and team communication. These competitions provide a hands-on learning experience, allowing students to explore real-world scenarios in a safe and controlled environment.

Solve Puzzles

Collaborate with your team to solve puzzles and advance to the next level

Crack Codes

Use your problem-solving skills to crack codes, decipher hidden clues, and unlock new hints that will guide you closer to your goal

Break Free

Use critical thinking to analyze, strategize, and break free from challenges

Academic Opportunities

Cybersecurity is a dynamic and multifaceted field that goes beyond just protecting computer systems—it safeguards individuals, businesses, and governments from digital threats. It encompasses areas like social engineering, where attackers exploit human psychology to gain unauthorized access to sensitive information; risk management, which helps organizations identify and mitigate potential security threats to their operations; and consumer privacy, ensuring individuals' personal data remains secure in an increasingly connected world. At Bradley University, students can study cybersecurity through multiple paths, such as the:

- Cybersecurity Major
- Cybersecurity Concentration within the Management Information Systems Major
- Cybersecurity Minor

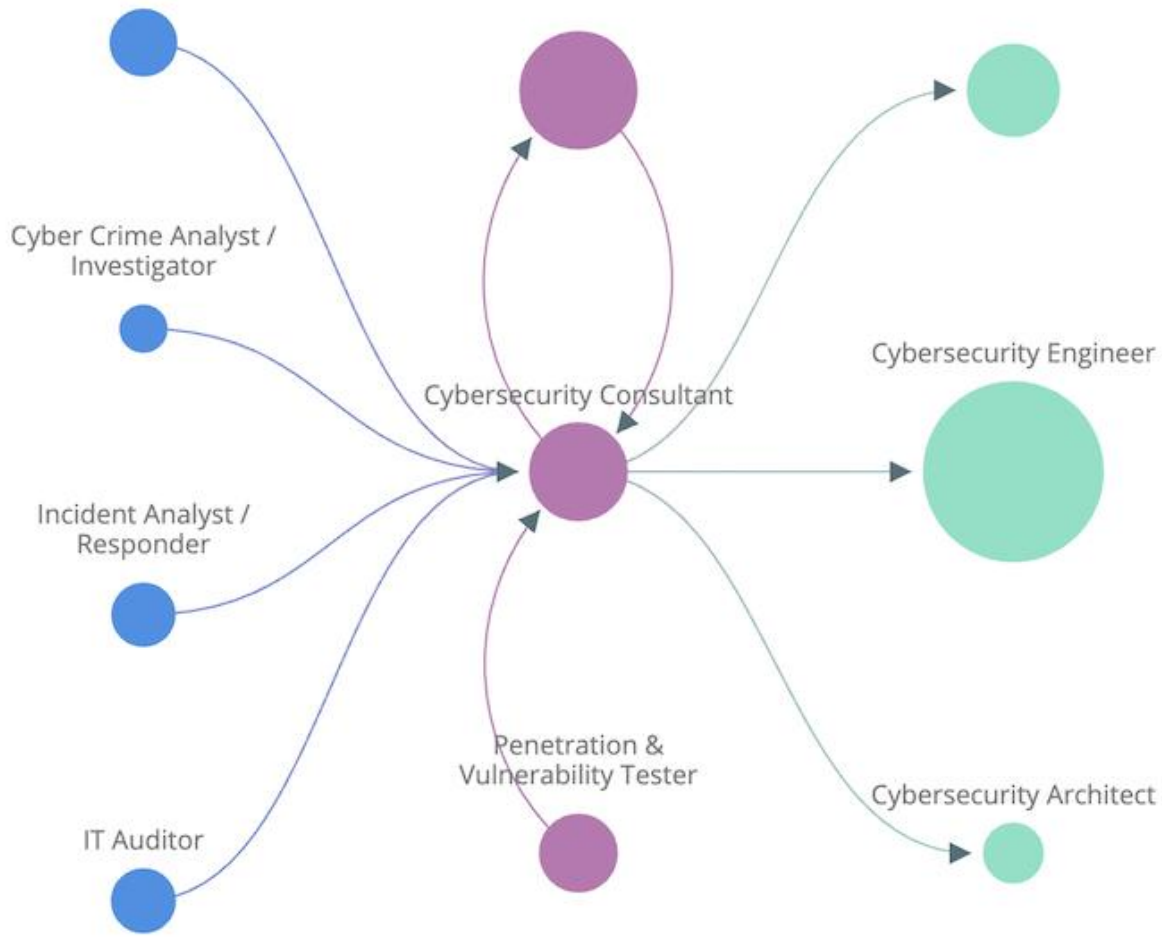
BRADLEY RED TEAM

Students at Bradley are able to participate in the most unique cybersecurity capstone experience in the country. As members of the Bradley Red Team, students perform a semester-long, full-scale, red teaming security assessment for a local business client through MIS 483: Advanced Ethical Hacking.

Assessment activities include:

- **Information Gathering:** researching websites and social media to find useful or exposed data
- **Social Engineering:** posing as utility workers, delivery drivers, and more to infiltrate the client
- **Network:** assessing client networks and systems to discover and exploit vulnerabilities
- **Physical:** using tools to ethically break-in to client facilities to demonstrate weaknesses

Careers in Cybersecurity



Cybersecurity jobs are in high demand now more than ever because cyberattacks are happening more often, technology is growing fast, and businesses need to protect their data and systems.

- There were 457,433 openings this year requesting cybersecurity-related skills
- From September 2023 through August 2024, there were only 83 cybersecurity workers available for every 100 cybersecurity jobs demanded by employers
- Cybersecurity workers protect our most important and private information, from bank accounts to sensitive military communications

Salaries for cybersecurity jobs vary based on the role, experience, location, and industry:

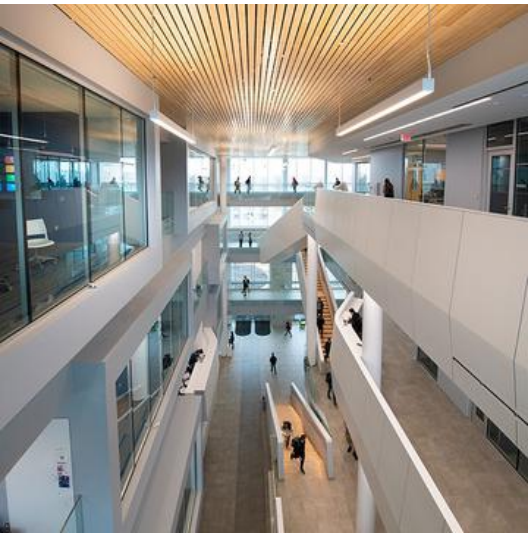
- **Entry-Level Roles** (ex: Cybersecurity Specialist, IT Auditor): $60,000 – $90,000
- **Mid-Level Roles** (ex: Cybersecurity Analyst, Penetration Tester): $90,000 – $130,000
- **Senior-Level Roles** (ex: Cybersecurity Architect, Cybersecurity Engineer): $130,000 – $180,000+
- **Executive Roles** (ex: Chief Information Security Officer): $200,000 – $400,000+

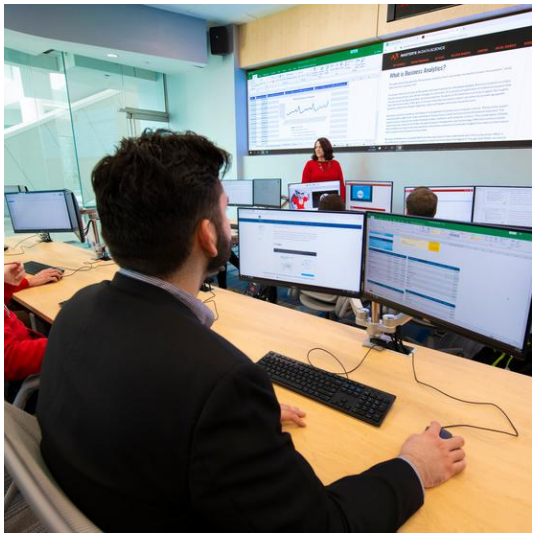
Business & Engineering Convergence Center

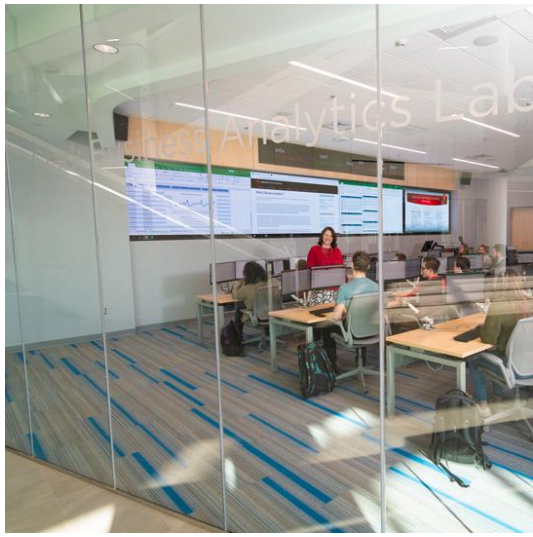
The Cyber 100 program will be held in the Business & Engineering Convergence Center (BECC) at Bradley University. The BECC is home to the Foster College of Business and the Caterpillar College of Engineering.

Business & Engineering Convergence Center
1500 West Main Street
Peoria, Illinois 61625

Logistical information will be shared later.







Code of Conduct

Cyber 100 promotes a respectful and inclusive environment. All participants are expected to adhere to the Code of Conduct. Failure to comply with these policies may result in removal from the event and notification to school officials.

Respect & Inclusion: Treat all attendees, speakers, and organizers with professionalism and respect. Discrimination, harassment, or inappropriate behavior will not be tolerated.

Photo & Video: Please do not take any photos or videos without permission. If anyone asks you to delete a photo or video of them, please do so.

Integrity & Ethics: Participants must adhere to ethical cybersecurity practices. Any attempts to compromise event security, disrupt sessions, or engage in unethical hacking will result in immediate disqualification and removal.

Compliance with Event Rules: Follow all instructions provided by event organizers, speakers, and workshop leaders. Any violations of event policies, including cheating in competitions, will lead to disqualification.

Privacy & Data Protection: Participants should respect the privacy of others and refrain from sharing personal or confidential information. The unauthorized collection or distribution of attendee data is strictly prohibited.

Participation & Engagement: Attendees should actively participate in discussions, workshops, and competitions while maintaining a positive and supportive environment.

Safety & Security: Cyber 100 is a safe learning space. Any actions that threaten the physical or digital security of attendees, including cyberbullying, hacking attempts, or disruptions, will be addressed with immediate consequences.

Use of Technology: Devices should be used responsibly. Unauthorized access to systems, tampering with equipment, or inappropriate use of event technology is not allowed.

Frequently Asked Questions

Who can participate in Cyber 100?
Any high school junior currently enrolled in a high school in the Peoria metropolitan area who has been nominated by a teacher, counselor, or staff member can participate.

Do students need someone to join them?
Yes, students must have a representative from their school attend with them. However, each representative can accompany multiple students.

Is there a fee for participation?
No, Cyber 100 is a free event for nominated students and their representative.

What should I bring to the event?
A willingness to learn! Everything that you need to participate will be provided, but you are welcome to bring your own materials.

Will meals be provided?
Yes, lunch and snacks will be provided for all participants. Dietary restrictions will be requested from participants upon acceptance to Cyber 100.

How can I prepare for the competition?
Participating in capture the flag (CTF) style competitions or escape rooms, and solving challenges like brain teasers could help!

How will the competition teams be formed?
The organizers will assign each team, but students from the same school will be kept together.

For any other inquiries related to Cyber 100, please reach out to:

Dr. Jacob Young
jayoung@bradley.edu

BRADLEY University

Center for Cybersecurity

bradley.edu/cybersecurity
centerforcybersecurity@bradley.edu
@BradleyCybersec