Module name: Fundamentals of cybersecurity – transdisciplinary approach.

Module teacher (e-mail)

Rafał T. Prabucki, PhD (rafal.prabucki@us.edu.pl)

Mateusz Jakubik, MA

Number of the ECTS credits

3 ECTS

Learning outcomes of the module

1. Problem-Solving:

- Apply critical thinking and problem-solving skills to address complex cybersecurity challenges.

- Develop and implement effective solutions to mitigate identified risks.

2. Communication:

- Communicate cybersecurity concepts, risks, and solutions effectively to both technical and non-technical stakeholders.

- Prepare comprehensive reports and documentation for security incidents, assessments, and audits.

3.Ethical and Professional Practices:

- Demonstrate ethical behavior and professional practices in the field of cybersecurity.

- Understand the ethical implications of cybersecurity decisions and actions.

4. Continuous Learning:

- Recognize the importance of staying current with evolving cybersecurity threats, technologies, and best practices.

- Engage in continuous learning through professional development, certifications, and research.

Maximum number of student who can take part in the module:	30

Co-funded by the European Union

Content of the module by chapter	1. Fundamental Concepts: - Understand the basic principles and concepts of cybersecurity, including confidentiality, integrity, and availability. - Explain the various types of cyber threats, vulnerabilities, and attack vectors. 2. Security Policies and Governance: - Understand the role of security policies, procedures, and governance in managing cybersecurity risks. - Recognize the importance of compliance with legal, regulatory, and organizational requirements in cybersecurity. 3. Cryptography: - Explain the principles of cryptography, including encryption, decryption, digital signatures, and key management. - Understand the differences between symmetric and asymmetric encryption and their appropriate use cases. 4. Types of Threats: - Identify and understand different types of cyber threats, including malware, ransomware, phishing, social engineering, denial-of-service attacks, and advanced persistent threats. - Understand the motivations and methods of cyber adversaries, including hackers, cybercriminals, and nation-state actors.
Module description	The main aim of the module:
	The primary aim of the cybersecurity module is to equip students with a comprehensive understanding of cybersecurity principles, practices, and technologies. This includes the ability to identify, analyze, and mitigate cyber threats and vulnerabilities, ensuring the protection of information systems and data. The module aims to develop both the theoretical knowledge and practical skills necessary for students to effectively manage and implement cybersecurity measures in various organizational contexts, fostering a culture of security awareness and ethical practices.

Module description	Subject area:
	Law / Privacy / Cybersecurity
	Target group:
	any interested students
	other:
	Field of study:
	any interested students
	other:
Assessment of the learning outcomes of the module	Type
	Cafeteria work assessment (select from the list): ☐ project ☒ test ☐ presentation ☐ poster presentation ☐ study results ☐ written assignment ☐ oral assignment ☐ other
	Description:
	The cybersecurity module test is designed to evaluate students' understanding and application of key cybersecurity concepts, principles, and practices. The test comprises a combination of multiple-choice questions, short answer questions, and practical scenarios to assess theoretical knowledge and practical skills. Students will be required to demonstrate their ability to identify and analyze cyber threats, apply security measures, and respond to cybersecurity incidents.

<table>
<tr><td rowspan="1"><b>Assessment of the learning outcomes of the module</b></td><td colspan="3"><b>Test Components:</b>
1. Multiple-Choice Questions (MCQs):
Assess knowledge of fundamental cybersecurity concepts, including types of threats, cryptographic principles, and security policies.
Test understanding of network security, operating system security, and application security.
2. Short Answer Questions:
Evaluate the ability to explain and elaborate on key cybersecurity principles and practices.
Assess understanding of security governance, risk management, and compliance requirements.
3. Practical Scenarios:
Present real-world cybersecurity scenarios for students to analyze and provide appropriate responses.
Assess practical skills in threat analysis, incident response, and the use of security tools and techniques.</td></tr>
<tr><td rowspan="7"><b>Forms of teaching</b></td><td>Type (select from the list):</td><td>Description (including teaching methods)</td><td>Number of hours
<b>In total = 24 hours</b></td></tr>
<tr><td>☒ lectures</td><td></td><td>10h</td></tr>
<tr><td>☐ seminars</td><td></td><td></td></tr>
<tr><td>☐ laboratory classes</td><td></td><td></td></tr>
<tr><td>☒ practical classes</td><td></td><td>8h</td></tr>
<tr><td>☒ online meeting</td><td></td><td>6h</td></tr>
<tr><td>☐ other:...............................</td><td></td><td></td></tr>
</table>

Student's own work	Description:	Number of hours **In total = minimum 51 hours**
	Before the classes in Katowice: To ensure that students are well-prepared for the cybersecurity module, it is essential for them to complete certain preparatory activities before the classes begin. This will help them gain a basic understanding of key concepts and terminology, allowing them to engage more effectively with the course material: **1. Reading Assignments,** **2. Software Installation**	10
	During the classes in Katowice: The cybersecurity module in Katowice will include a blend of theoretical lessons, practical exercises, group activities, and guest lectures. The objective is to ensure that students gain both knowledge and hands-on experience in cybersecurity.	30
	After the classes in Katowice: Upon completing the cybersecurity module in Katowice, students should continue their learning and professional development to reinforce and expand upon the knowledge and skills acquired during the course.	11
Module literature, obligatory reading	Description:	
	Module Literature: Obligatory Reading for Cybersecurity Module To provide a strong foundation in cybersecurity principles and practices, the following books and resources are considered essential reading for the cybersecurity module. These texts cover a broad range of topics, including fundamental concepts, threat analysis, risk management, and practical applications.	

Module literature, obligatory reading	**Obligatory Reading:** 1. **"Cybersecurity Essentials" by Charles J. Brooks, Christopher Grow, Philip Craig, and Donald Short** ○ **Description:** This comprehensive guide covers the fundamental concepts of cybersecurity, including threat landscapes, risk management, and security frameworks. It is suitable for both beginners and those looking to refresh their knowledge. ○ **Topics Covered:** Basic cybersecurity principles, security policies, risk management, network security, cryptography, and incident response. 2. **"Network Security Essentials: Applications and Standards" by William Stallings** ○ **Description:** This book provides a detailed introduction to network security principles and applications. It covers essential topics such as cryptographic algorithms, authentication protocols, and secure network design. ○ **Topics Covered:** Cryptography, authentication, network security protocols, wireless network security, and intrusion detection. 3. **"The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard and Marcus Pinto** ○ **Description:** This practical guide focuses on web application security, teaching readers how to identify and exploit common vulnerabilities. It is ideal for students interested in penetration testing and ethical hacking. ○ **Topics Covered:** Web application vulnerabilities, SQL injection, cross-site scripting (XSS), authentication and session management, and security testing tools.

Co-funded by the European Union

Module literature, obligatory reading	4. **"Security Risk Management: Building an Information Security Risk Management Program from the Ground Up" by Evan Wheeler** ○ **Description:** This book provides a comprehensive approach to building and managing an information security risk management program. It is essential for understanding how to assess and mitigate risks in an organizational context. ○ **Topics Covered:** Risk assessment methodologies, risk mitigation strategies, security policies, and governance frameworks. 5. **"Applied Cryptography: Protocols, Algorithms, and Source Code in C" by Bruce Schneier** ○ **Description:** A classic text on cryptography, this book covers a wide range of cryptographic techniques and their applications. It includes practical examples and source code for implementing cryptographic algorithms. ○ **Topics Covered:** Symmetric and asymmetric encryption, cryptographic protocols, key management, digital signatures, and cryptographic applications. 6. **"Incident Response & Computer Forensics" by Chris Prosise and Kevin Mandia** ○ **Description:** This book provides a detailed look at incident response and digital forensics. It covers methodologies for detecting, responding to, and investigating cyber incidents. ○ **Topics Covered:** Incident response planning, forensic analysis techniques, evidence collection, and handling, and real-world case studies. **Recommended Journals and Articles:**

Module literature obligatory reading	• **"IEEE Security & Privacy" Journal** ○ **Description:** A leading journal that publishes cutting-edge research and articles on a wide range of cybersecurity topics. ○ **Topics Covered:** Latest research findings, case studies, industry trends, and expert opinions on various aspects of cybersecurity. • **"ACM Transactions on Privacy and Security (TOPS)"** ○ **Description:** This journal features high-quality research papers on privacy and security in computer systems and networks. ○ **Topics Covered:** Security mechanisms, cryptographic methods, privacy-enhancing technologies, and security protocols. **Online Resources:** • **National Institute of Standards and Technology (NIST) Cybersecurity Framework** ○ **Description:** A comprehensive framework that provides guidelines for managing cybersecurity risks. ○ **Topics Covered:** Core functions, categories, and subcategories for cybersecurity risk management, best practices, and implementation guidelines. • **Open Web Application Security Project (OWASP)** ○ **Description:** A non-profit organization focused on improving software security. OWASP provides numerous resources, including the OWASP Top 10 list of web application vulnerabilities. ○ **Topics Covered:** Web application security risks, secure coding practices, and security testing tools.

Technical requirements and teaching aids necessary for conducting classes at University of Silesia
Equipment provided by the foundation (no-cost), board-play (if you manage to buy through the university)
Minimum attendance requirement
1