Cyber Security

26HS

Programme	BSc in Business Artificial Intelligence
Degree	Bachelor
ECTS	6
Module type	elective module
Module coordinator	Hermann Grieder
Leading principle / Short description	Digitalization creates new requirements for protecting digital assets against evolving threats. While IT security encompasses a broad spectrum of protection measures, cybersecurity specifically focuses on defending systems, networks, and programs from digital attacks. As cyber threats become more sophisticated, the need for specialized knowledge in this area is critical across all industries. In this module, participants acquire knowledge about cyber threat landscapes, attack vectors, and defensive approaches. Advanced concepts for protecting against targeted attacks as well as selected techniques for practical implementation of cyber defense mechanisms are taught.
Module content	This module conveys fundamental concepts of cybersecurity and their interactions with artificial intelligence in modern business environments. Students develop an understanding of how AI can function both as a security tool and as a potential attack instrument. The course also looks at the privacy and legal aspects at the intersection of AI and cybersecurity in the business context.
Competencies to be achieved	**Knowledge and Understanding:** ***The students...*** ○ Understand cybersecurity as a specialized discipline requiring constant vigilance and adaptation ("Cyber Awareness") ○ Know typical cyber-attack vectors including social engineering, malware, phishing, and advanced persistent threats ("Cyber Threat Landscape") ○ Know selected cybersecurity frameworks and compliance requirements, can differentiate between them and identify their application in various contexts ("Cybersecurity Governance") ○ Understand attack methodologies and techniques used by threat actors including exploitation of vulnerabilities and breach mechanisms ("Cyber Attack Vectors") ○ Know defensive strategies from both offensive and defensive security perspectives ("Practical Cyber Defense") **Application of Knowledge and Understanding:** ***The students...*** ○ Can identify and classify common types of cyber threats through guided exercises and case studies ○ Can implement basic security measures such as strong password policies and multi-factor authentication ○ Can perform security assessments to identify obvious vulnerabilities in systems ○ Can use basic security tools to monitor and detect suspicious activities ○ Can follow established incident response procedures for common cybersecurity incidents **Critical Thinking:** ***The students...*** ○ Can develop effective cybersecurity strategies based on threat intelligence and risk assessment ○ Can evaluate the effectiveness of various cybersecurity tools and approaches against different types of threats ○ Can analyze attack patterns and develop appropriate countermeasures for emerging cyber threats
Prerequisites	None
Teaching and learning methods	Contact Hours: Lecture, Seminar, Assignment, Discussion Guided Self-Study: Individual Work
Grading	Grade 1-6 (half grades)

Assessment

Exam 100%	
Oral / Written	Written
Duration (min)	90
Timeframe	examination period (end of semester)
Grading Scale	Points

Module details

Cyber Security - Fri - Olten	
Time	8:15 AM - 12:00 PM
Language	Deutsch
Max. participants	40
Periodicity	Weekly
Lecturers	Dr. Pascal Moriggl, Hermann Grieder
Number	3-26HS.W-B-BAI-000207.EN/WPM