Cyber Resilience

26FS

Programme	BSc in Wirtschaftsinformatik BSc in Business Information Technology
Degree	Bachelor
ECTS	5
Module type	elective module
Module coordinator	Prof. Dr. Petra Asprion
Compulsory attendance	Approx. 20% - announced on dates
Leading principle / Short description	Cyber resilience is crucial for organizations as it extends beyond cybersecurity and its prevention view. Cyber resilience focuses on the ability to continue operating during and recover from cyber threats. It involves preparing staff to handle potential cyber disruptions and maintaining system operations under attack, ensuring both organizational continuity and the protection of sensitive data. By embedding resilience strategies, organizations safeguard their assets, sustain customer trust, and mitigate financial losses, making resilience a fundamental aspect of comprehensive cybersecurity. The lecture is structured in three perspectives: ◦ Organizational View: Focuses on governance, risk management, and culture. It involves establishing clear policies, roles, and responsibilities across the organization to enhance resilience through training, awareness programs, and regular assessments of security practices. ◦ Technical View: Centers on the architecture and systems used to protect data and maintain operations. This includes the implementation of robust technologies along with continuous monitoring and rapid response to threats. ◦ Protection / Security First View: Prioritizes proactive security measures to prevent breaches before they occur.
Module content	1. Introduction to Cyber Resilience ◦ Definition and Scope: concept of cyber resilience, contrasting it with cybersecurity. ◦ Importance: Discuss the critical role of cyber resilience in ensuring operational continuity, protecting sensitive data, and maintaining trust. 2. Organizational View ◦ Governance, risk management, and culture: it involves establishing clear policies, roles, and responsibilities. ◦ Cultural Impact: organizational culture on cyber resilience, security awareness and training programs. ◦ Case Studies and Examples: real-world examples of organizations that successfully implemented robust governance frameworks and cultural shifts. 3. Technical View ◦ System Architecture and Data Protection: technical infrastructure necessary for protecting data and maintaining operations. ◦ Continuous Monitoring and Rapid Response: technologies and processes for ongoing threat monitoring. ◦ Technological Innovations: recent advancements in technology that support cyber resilience, such as cloud security architectures and AI-driven security. 4. Protection/Security First View ◦ Proactive Security Measures: practice implementing of security measures. ◦ Secure by Design: Explain the concept of 'security by design' 5. Conclusion ◦ Synthesis: key points from each perspective, synthesizing how they interlink to enhance an organization's cyber resilience.

Competencies to be achieved

Knowledge and Understanding:
- Students understand the key principles of cyber resilience beyond basic cybersecurity.
- They recognize the importance of governance, risk management, and organizational culture in enhancing cyber resilience.
- Students are familiar with the organizational infrastructure necessary to protect data and ensure operational continuity.
- They understand proactive security measures and their role in preventing cyber breaches.

Applying Knowledge and Understanding:
- Students can apply their knowledge to evaluate and enhance organizational policies and practices for cyber resilience.
- They are capable of assessing and deploying technical solutions that support continuous monitoring and rapid response systems.

Judgements:
- Students can critically assess the effectiveness of current cybersecurity measures within an organization.
- They can make informed decisions regarding the implementation of governance and risk management strategies to enhance cyber resilience.
- Students are equipped to prioritize actions based on potential cyber threats and organizational vulnerabilities.

Communication Skills:
- Students can effectively communicate the importance of cyber resilience strategies to stakeholders within the organization.
- They can articulate complex cybersecurity concepts clearly to both technical and non-technical audiences.
- Students can advocate for continuous improvement in cybersecurity practices through training and awareness programs.

Learning Skills:
- Students are prepared to continuously update their knowledge in the fast-evolving field of cybersecurity and cyber resilience.
- They can independently seek out new technologies and methodologies to enhance organizational resilience.
- Students are motivated to participate in ongoing lear

Prerequisites

IT security module is strongly recommended

Teaching and learning methods

Contact studies: lecture, exercise, discussion, presentation, group work, case studies
Guided self-study: individual work, group work, literature study, project work, depending on agreement: videocast, podcast

Literature

Is made available on Moodle or referred to via link

Remarks

This module is part of the specialization Cybersecurity Management

Grading

Grade 1 - 6 (half grades)

Assessment

Moodle/ipad exam 60%	
Oral / Written	written
Duration (min)	60 min
Timeframe	During the examination period
Grading Scale	points
Remarks	A moodle or ipad assessment will be carried out
Group work 40%	
Oral / Written	written / presentation
Duration (min)	20 Min
Timeframe	As part of an event
Grading Scale	pints
Remarks	Group work is planned; each group member receives the same number of points.

Module details

Cyber Resilience (DBM/CSM) - Mon - Basel	
Time	1:15 PM - 5:00 PM
Language	Englisch
Max. participants	64
Periodicity	Weekly
Lecturers	Prof. Dr. Petra Asprion, Dr. Pascal Moriggl
Number	2-26FS.W-B-WIBIT-060712S1.SN/VR

Cyber Resilience (DBM/CSM) - Wed - Olten	
Time	1:15 PM - 5:00 PM
Language	Deutsch
Periodicity	Weekly
Lecturers	Prof. Dr. Petra Asprion, Dr. Pascal Moriggl, Dr. Felix Härer
Number	3-26FS.W-B-WIBIT-060732S1.SN/VR