Master of Science in Enterprise Cybersecurity
Fact Sheet

Overall Program Description

The integrity and security of data have emerged as the foundations of modern businesses in an age where digital connection is of utmost importance. There is a growing demand for individuals who can not only comprehend the complexities of cybersecurity but also bridge the gap between the technical complexities and wider business objectives as cyber threats become more complex. Technical expertise and business strategy must be balanced, although many businesses struggle to find such balance. This is mainly because domain experts may not have a thorough understanding of cybersecurity, and cybersecurity professionals may not always understand the larger business ramifications.

Students who envision themselves at the forefront of companies, working as the link between management and technological teams, should take advantage of OPIT's MSc in Enterprise Cybersecurity. Such individuals will play a key role in developing the cybersecurity strategy, interpreting threat assessments, and assisting leadership in making strategic decisions that secure digital assets and ensure organizational resilience.

The program's progression is divided into three distinct phases that correlate to the three terms:

Building solid foundations on cybersecurity with a focus on the growth of a corporate strategy, analytical acuity, and fundamental cybersecurity principles.

Transition from theoretical knowledge to practical application, delving deep into specialized cybersecurity areas. Augmented by elective options that allow for customized learning experiences and guest lectures that provide insights into real-world industries.

Consolidating what has been learnt through a capstone project and dissertation.

The key features of the proposed MSc in Enterprise Cybersecurity are:

Aligned with Industry Certifications: wherever possible, the Program’s modules are aligned with key industry certifications (such as CISSP, CISM, and CRISC), providing students not just with a strong applicative knowledge on today’s cybersecurity, but also with conceptual and practical knowledge that will allow them to pursue such certifications;

Balanced Curriculum: The program offers a balanced mix of technical knowledge, managerial/strategic knowledge, and soft skills, making it unique in its comprehensive approach to cybersecurity education;

Modular Structure: The program is built considering three exit points leading to three different degrees of increasing value (Post graduate Certificate, Post graduate Diploma, and Masters of Science) offering maximum flexibility to students depending on their needs;

Real-world Application: The capstone project provides an opportunity for practical application of skills, ensuring that students are job-ready upon graduation.

The program has multiple exit paths (see more details in Section "Exit Awards/Qualifications"), offering 60 ECTS of taught modules and a Capstone Project and Dissertation module that is worth either 30 or 60 ECTS. Before the beginning of the Capstone Project and Dissertation module, the students must select either the 30 or the 60 ECTS instance of the module, and their choice will be recorded in appropriate internal documentation. Their effort and time commitment to complete the module will be suitably calibrated by the supervisors according to their choice.

Target Audience

Ages 19 – 30	☒	Age 31 – 65	☒
Age 65+	☒		

Target Group

OPIT's MSc in Enterprise Cybersecurity is built for:

- Students who might not have a foundational background in technology or security but are looking to pivot their careers into the realm of Cybersecurity.
- Professionals who are in the quest to enhance their skill set by developing a "holistic" understanding and robust management abilities in the domain of Cybersecurity tailored to contemporary digital challenges.

The ultimate purpose of this programme is to connect students from varied backgrounds and demonstrate how Cybersecurity methodologies and tools can be applied across diverse sectors.

To ensure that this program is welcoming to those without a foundational technical understanding, it has been curated such that no preliminary technical knowledge is mandated. However, to smooth the transition and make the program more accessible to those less acquainted with technology, OPIT will grant them complimentary, optional access to educational resources aimed at bridging potential foundational gaps. This additional content will be available in an asynchronous format (comprising videos, exercises, and reference materials) via the Virtual Learning Environment, during the summer Term preceding the commencement of the MSc program. To elucidate further, OPIT will unveil modules like ICT Fundamentals and Introduction to Cybersecurity. These modules are intended to equip students from non-technical disciplines (for instance, Humanities) with the requisite foundational understanding. Additionally, the technical modules in the inaugural term of the MSc program are meticulously designed to gradually familiarize students with more advanced Cybersecurity topics to be delved into later in the curriculum.

The MSc programme's main goal is to cultivate professionals who are adept at liaising both with organizational leadership and technical teams in corporate settings or research institutions. Upon the program's completion, graduates will be positioned to integrate into companies or research entities, serving as the pivotal link between managerial and technical factions, steering the cybersecurity strategy, interpreting security analyses, and aiding leadership in making informed, security-centric decisions.

Entry Requirements

The admission requests from new applicants are received by the Students Secretary Office, which will conduct an interview with the applicants.

Students will need to provide the following documents for admission:

1. Updated CV in English;
2. Copy of a valid ID (front and back);

Qualifications:

3. University degrees (MQF level 6 or higher) in STEM fields (Science, Technology, Engineering, Mathematics), Business Administration, Information Security, Law, Liberal Arts, Medical Sciences, Humanities.

Since all OPIT programs are taught in English, a proof of language proficiency is needed. Any of the following options is accepted as a proof of English proficiency:

1. Being a English native speaker;
2. Having completed a previous degree entirely taught in English;
3. Having passed one of the following English tests:
    - TOEFL (minimum 80 points)
    - IELTS (minimum Level 6)
    - Duolingo English Test (minimum 95 points)
    - Cambridge Certificate (minimum B2 grade overall)

Students, who do not hold the requested level must sit for the English Entry Test in order to certify the students' competences.

All the enrolled students will follow an Induction Module before the beginning of the chosen training. This will explain to the student all the policies and procedures outlined in this handbook, and specific information related to the training, such as learning outcomes and expectations.
Study Guidelines will also be shared. Induction will also include a handbook and/or a tutorial lesson related to the different functionalities of the Virtual Learning Environment and how to use it. If students have any specific requirements or needs, they should inform the Students Support Office.

During the admission process of students wishing to enroll to the program, we will also ensure that such students have the required basic digital competence to successfully complete such a course. We will do so by administering to such students a standardized questionnaire that will cover aspects including, but not limited to: the availability of a PC with a webcam and speakers, the availability of an adequate internet connection, basic knowledge of operating systems and web browsers.

To fully align with the program's learning objectives, students are required to have some technical proficiency (in terms of basic information technology skills) and some preliminary understanding of modern cybersecurity. However, the program offers an entry path that allows to fill possible gaps in terms of such requirements (e.g. for students coming from Business, Law, Liberal Arts, Medical Sciences, Humanities).

Direct Entry: At least a BSc from an accredited institution with a substantial information technology background and some knowledge of cybersecurity. Notably, in their previous degrees, candidates applying under the Direct Entry path will have passed courses equivalent to the following OPIT's courses:
COMP-1005 ICT Fundamentals
COMP-4005 Introduction to Computer Security

Alternative Entry: Applicants who hold degrees (at least a BSc) but without technical skills or with technical skills yet not directly related to cybersecurity can apply under the Alternative Entry path. In order to ensure success in the program, such applicants will be required to undergo specialized assessments to evaluate their foundational skills. The Basic Competencies Assessment (BCA) will be based on the following preparatory modules taken from OPIT programs, which are offered free of charge during summer, before the start of the first Term:
COMP-1005 ICT Fundamentals
COMP-4005 Introduction to Computer Security

The BCA consists of a test with a mix of multi-choice and open-ended questions. If a student fails more than 50% of the questions, the test is considered as failed. Students not clearing the BCA will have an opportunity for a retake after a dedicated period of remedial guidance, within the same academic year.

Recognition of Prior Learning
OPIT recognizes previous academic and professional experience in different ways. Procedures that describe the mechanisms related to admission and RPL are entirely described at the following webpage:

https://www.opit.com/fee-admission/

Learning Outcomes for Knowledge obtained at the end of the programme

The learner will be able to:

a) Bookmark and recall foundational cybersecurity principles and their relevance in contemporary digital ecosystems
b) Highlight and describe critical cybersecurity terminologies and their applications in threat detection
c) Identify prevalent cyber threats in sectors like Banking, Healthcare, and E-commerce
d) Spread cybersecurity-related knowledge in workshops and via other communication channels, providing insights on the applicability of established cybersecurity measures in various IT settings
e) Search and list vulnerabilities linked to specific digital tools and platforms
f) Comment on the implications of breaches by referencing real-world cybersecurity incidents
g) Link different cyber threats with their countermeasures, drawing from industry scenarios
h) Subscribe to and quote international cybersecurity standards and best practices
i) Link and sequence a cybersecurity audit's components, detailing the steps for businesses
j) Write clear explanations, translating intricate cybersecurity challenges for a broader audience

Learning Outcomes for Skills obtained at the end of the programme

The learner will be able to:

a) Apply cybersecurity protocols to safeguard digital assets within a business environment
b) Design comprehensive cybersecurity strategies tailored to specific industry needs, integrating best practices
c) Construct a robust cybersecurity framework, drawing from real-world threat scenarios and mitigation techniques
d) Demonstrate proficiency in using advanced cybersecurity tools and software by troubleshooting simulated cyber incidents
e) Plan and arrange cybersecurity audits for organizations, ensuring comprehensive threat detection and vulnerability assessment
f) Compose detailed cybersecurity reports, synthesizing complex data and findings into actionable recommendations
g) Practice ethical hacking techniques in controlled environments to understand potential vulnerabilities and strengthen security postures
h) Create and assemble training modules to educate non-technical staff about cybersecurity best practices and threat awareness
i) Operate and use various cybersecurity platforms and technologies, ensuring optimal security configuration for diverse digital assets
j) Prepare contingency plans and response strategies to address potential cyber breaches, ensuring swift recovery and minimal data loss

30 ECTS

Hours of Total Learning 1 ECTS is equivalent to 25 total hours of learning, inclusive of contact hours, supervised placement and practice hours, self-study hours and assessment hours.	Total Contact Hours [1] 168 (Contact Hours are hours invested In learning new content under the Direction of a tutor/lecturer (e.g. lectures, participation in online forums, video-lectures)	Supervised Placement and Practice Hours 168 (During these hours the learner is supervised, coached, or mentored. Tutorial hours may be included here)
	Self-Study Hours 369 (Estimated workload of research and study)	Assessment Hours 45 (Examinations/ presentations/ group work/ projects, etc.)
Total Learning Hours	**750 Hours**	

60 ECTS

Hours of Total Learning 1 ECTS is equivalent to 25 total hours of learning, inclusive of contact hours, supervised placement and practice hours, self-study hours and assessment hours.	Total Contact Hours [2] 336 (Contact Hours are hours invested In learning new content under the Direction of a tutor/lecturer (e.g. lectures, participation in online forums, video-lectures)	Supervised Placement and Practice Hours 336 (During these hours the learner is supervised, coached, or mentored. Tutorial hours may be included here)
	Self-Study Hours 738 (Estimated workload of research and study)	Assessment Hours 90 (Examinations/ presentations/ group work/ projects, etc.)
Total Learning Hours	**1500 Hours**	

[1] *In the case of online learning, synchronous and asynchronous learning activities under the direction and control of an instructor are considered as contact hours.*

[2] *In the case of online learning, synchronous and asynchronous learning activities under the direction and control of an instructor are considered as contact hours.*

90 ECTS

Hours of Total Learning 1 ECTS is equivalent to 25 total hours of learning, inclusive of contact hours, supervised placement and practice hours, self-study hours and assessment hours.	Total Contact Hours [3] 504 (Contact Hours are hours invested In learning new content under the Direction of a tutor/lecturer (e.g. lectures, participation in online forums, video-lectures)	Supervised Placement and Practice Hours 504 (During these hours the learner is supervised, coached, or mentored. Tutorial hours may be included here)
	Self-Study Hours 1107 (Estimated workload of research and study)	Assessment Hours 135 (Examinations/ presentations/ group work/ projects, etc.)
Total Learning Hours	**2250 Hours**	

120 ECTS

Hours of Total Learning 1 ECTS is equivalent to 25 total hours of learning, inclusive of contact hours, supervised placement and practice hours, self-study hours and assessment hours.	Total Contact Hours [4] 690 (Contact Hours are hours invested In learning new content under the Direction of a tutor/lecturer (e.g. lectures, participation in online forums, video-lectures)	Supervised Placement and Practice Hours 640 (During these hours the learner is supervised, coached, or mentored. Tutorial hours may be included here)
	Self-Study Hours 1540 (Estimated workload of research and study)	Assessment Hours 130 (Examinations/ presentations/ group work/ projects, etc.)
Total Learning Hours	**3000 Hours**	

[3] *In the case of online learning, synchronous and asynchronous learning activities under the direction and control of an instructor are considered as contact hours.*

[4] *In the case of online learning, synchronous and asynchronous learning activities under the direction and control of an instructor are considered as contact hours.*

The Program Structure

Module/ Unit Title	Compulsory (C) or Elective (E)	ECTS	MQF Level	Mode of Teaching	Mode of Assessment	Term
Cybersecurity Fundamentals and Governance	Compulsory	6	7	Live lectures, asynchronous contents	Exercises, Tests	1
Network Security and Intrusion Detection	Compulsory	6	7	Live lectures, asynchronous contents	Exercises, Tests	1
Legal Aspects and Compliance	Compulsory	6	7	Live lectures, asynchronous contents	Exercises, Tests	1
Cryptography and Secure Communications	Compulsory	6	7	Live lectures, asynchronous contents	Exercises, Tests	1
Data Analytics and Risk Management	Compulsory	6	7	Live lectures, asynchronous contents	Exercises, Tests	1
Generative AI in Cybersecurity	Compulsory	6	7	Live lectures, asynchronous contents	Exercises, Tests	2
Business Resilience and Response Strategies	Compulsory	6	7	Live lectures, asynchronous contents	Exercises, Tests	2
Behavioral Cybersecurity	Elective	6	7	Live lectures, asynchronous contents	Exercises, Tests	2
Cloud and IoT Security	Elective	6	7	Live lectures, asynchronous contents	Exercises, Tests	2
Secure Software Development	Elective	6	7	Live lectures, asynchronous contents	Exercises, Tests	2
Critical Thinking and Problem-Solving	Elective	6	7	Live lectures, asynchronous contents	Exercises, Tests	2
Leadership & Communication in Cybersecurity	Elective	6	7	Live lectures, asynchronous contents	Exercises, Tests	2
AI-Driven Forensic Analysis in Cybersecurity	Elective	6	7	Live lectures, asynchronous contents	Exercises, Tests	2
Capstone Project and Dissertation - for students completing MSc at 90 ECTS	Compulsory	30	7	-	Project, Dissertation	3
Capstone Project and Dissertation - for students completing MSc at 120 ECTS	Compulsory	60	7	-	Project, Dissertation	3 - 4
Total ECTS for Program Completion		**30/60/90/120 ECTS**				

Cybersecurity Fundamentals and Governance
Compulsory
6 ECTS
Term 1

Course Description

This foundational course provides a comprehensive overview of cybersecurity, focusing on risk management, security technologies, and governance policies. The course is designed to equip students with the knowledge and skills they need to understand the complex landscape of cybersecurity and to make informed decisions related to security governance.

Tentative list of topics:

- Introduction to Cybersecurity: Key concepts and terminologies
- Risk Management in Cybersecurity: Risk assessment and mitigation strategies
- Security Policies and Procedures: Development and implementation
- Governance Frameworks: Overview and application in cybersecurity
- Compliance and Legal Requirements: Laws, regulations, and compliance frameworks
- Case Studies and Real-world Applications: Analysis of real-world cybersecurity incidents

Applying Knowledge and Understanding

At the end of the module/unit the learner will have acquired the following skills:

a) Analyze real-world cybersecurity incidents
b) Apply risk assessment techniques in cybersecurity scenarios
c) Create effective security governance policies

Module-Specific Learner Skills

At the end of the module/unit the learner will be able to

a) Apply governance policies and frameworks in cybersecurity contexts
b) Design risk management strategies tailored to specific cybersecurity threats
c) Demonstrate a comprehensive understanding of the cybersecurity landscape

Module-Specific Digital Skills and Competences

At the end of the module/unit, the learner will be able to

a) Use digital platforms to monitor and manage security governance
b) Operate tools for risk assessment and mitigation in cybersecurity
c) Arrange and present cybersecurity data in dashboards for decision-making

⭡ Back to the Programme Structure

Network Security and Intrusion Detection
Compulsory
6 ECTS
Term 1

Course Description

This course dives deep into the world of network security, addressing the various threats networks face and the solutions to detect and counteract them. It explores intrusion detection systems, network vulnerabilities, and the techniques to safeguard network infrastructures.

Tentative list of topics:

- Network Security Basics: Protocols, topologies, and devices
- Vulnerabilities and Attack Vectors: Common threats to network infrastructures
- Intrusion Detection Systems: Types, techniques, and implementations
- Preventive and Reactive Measures: Firewalls, VPNs, and other countermeasures
- Case Studies: Real-world network attacks and responses

Applying Knowledge and Understanding

At the end of the module/unit the learner will have acquired the following skills:

a) Apply techniques to safeguard network infrastructures
b) Monitor and respond to potential network attacks
c) Design robust network security architectures

Module-Specific Learner Skills

At the end of the module/unit the learner will be able to

a) Design secure network architectures resistant to common threats
b) Apply intrusion detection mechanisms to monitor and respond to threats
c) Demonstrate expertise in securing both wired and wireless networks

Module-Specific Digital Skills and Competences

At the end of the module/unit, the learner will be able to

a) Use network monitoring tools to detect and respond to intrusions
b) Operate firewall configurations and VPN setups for secure connections
c) Assemble network logs for analysis and threat detection

⭡ Back to the Programme Structure

Legal Aspects and Compliance

Compulsory
6 ECTS
Term 1

Course Description

The course provides an understanding of the legal landscape surrounding cybersecurity. It discusses regulations, laws, and compliance measures that organizations must be aware of to maintain a secure and legally compliant cyber environment.

Tentative list of topics:

- Cyber Laws and Regulations: International and local perspectives
- Compliance Frameworks: Standards and guidelines for cybersecurity
- Legal Implications of Cyber Attacks: Liabilities and litigations
- Data Protection and Privacy: Laws governing data usage and storage
- Case Studies: Legal challenges in real-world cybersecurity incidents

Applying Knowledge and Understanding

At the end of the module/unit the learner will have acquired the following skills:

a) Analyze legal challenges in real-world cybersecurity scenarios
b) Apply knowledge of laws to assess organizational cybersecurity posture
c) Navigate legal frameworks to ensure cybersecurity compliance

Module-Specific Learner Skills

At the end of the module/unit the learner will be able to

a) Apply legal frameworks and regulations relevant to cybersecurity
b) Design compliance strategies for businesses operating in the digital domain
c) Demonstrate understanding of the legal implications of cybersecurity breaches

Module-Specific Digital Skills and Competences

At the end of the module/unit, the learner will be able to

a) Use digital repositories to stay updated on evolving cybersecurity laws.
b) Operate compliance management tools tailored for cybersecurity.
c) Arrange digital documentation for legal audits and compliance checks.

⬆ Back to the Programme Structure

Cryptography and Secure Communications

Compulsory
6 ECTS
Term 1

Course Description

This course delves into the realm of cryptography, shedding light on the techniques that enable secure communications. It discusses encryption methodologies, key management, and how cryptography is used to safeguard data during transit and rest.

Tentative list of topics:

- Basics of Cryptography: Symmetric vs. asymmetric, public key infrastructure
- Encryption Algorithms: DES, AES, RSA, and modern techniques
- Secure Communications Protocols: SSL, TLS, and beyond
- Key Management: Generation, distribution, and storage
- Case Studies: Real-world applications of cryptography

Applying Knowledge and Understanding

At the end of the module/unit the learner will have acquired the following skills:

a) Apply cryptographic techniques to ensure data security.
b) Design systems that use secure communication protocols.
c) Analyze cryptographic challenges and devise solutions.

Module-Specific Learner Skills

At the end of the module/unit the learner will be able to

a) Design secure communication protocols using cryptographic principles
b) Apply encryption and decryption methods for data protection
c) Demonstrate expertise in public and private key infrastructures

Module-Specific Digital Skills and Competences

At the end of the module/unit, the learner will be able to

a) Use encryption tools for secure data storage and transit
b) Operate cryptographic libraries and frameworks for software development
c) Arrange secure communication channels in a networked environment

🠅 Back to the Programme Structure

Data Analytics and Risk Management
Compulsory
6 ECTS
Term 1

Course Description

The course focuses on utilizing data analytics in cybersecurity for risk assessment and management. It covers techniques to analyze vast amounts of data to detect threats, understand vulnerabilities, and make informed risk-related decisions.

Tentative list of topics:

- Introduction to Data Analytics in Cybersecurity
- Risk Assessment Techniques: Identifying and quantifying risks
- Data-Driven Threat Detection: Machine learning and AI in threat detection
- Risk Mitigation Strategies: Data-informed decision making
- Case Studies: Using data analytics in real-world cybersecurity scenarios

Applying Knowledge and Understanding

At the end of the module/unit the learner will have acquired the following skills:

a) Analyze vast datasets to detect potential security threats
b) Apply data analytics techniques to inform risk-related decisions
c) Design and implement machine learning models for cybersecurity applications

Module-Specific Learner Skills

At the end of the module/unit the learner will be able to

a) Design data-driven risk assessment strategies for cybersecurity
b) Apply data analytics techniques to decipher cybersecurity threats
c) Demonstrate the ability to make informed decisions based on cyber data insights

Module-Specific Digital Skills and Competences

At the end of the module/unit, the learner will be able to

a) Use data analytics platforms to process and analyse cybersecurity data.
b) Operate risk management tools tailored for cyber environments.
c) Arrange digital reports highlighting cyber risk and mitigation strategies.

⬆ Back to the Programme Structure

Generative AI in Cybersecurity
Compulsory
6 ECTS
Term 2

Course Description

This advanced course delves into the role of AI in shaping the future of cybersecurity. It covers techniques to utilize generative AI models for security solutions and threat detection. Students will gain insights into the potential and challenges of using AI in cybersecurity applications.

Tentative list of topics:

- Introduction to Generative AI: Concepts and Applications
- AI in Threat Detection: Techniques and Challenges
- Application of Generative Models in Cybersecurity
- AI-Driven Security Solutions: Case Studies
- Ethical Implications of AI in Cybersecurity

Applying Knowledge and Understanding

At the end of the module/unit the learner will have acquired the following skills:

a) Design AI-driven security solutions
b) Analyze the effectiveness of AI in real-world cybersecurity scenarios
c) Implement AI models and tools to enhance cybersecurity posture

Module-Specific Learner Skills

At the end of the module/unit the learner will be able to

a) Apply AI algorithms to generate cybersecurity solutions
b) Design AI-driven threat detection mechanisms
c) Demonstrate an understanding of ethical considerations in AI for cybersecurity

Module-Specific Digital Skills and Competences

At the end of the module/unit, the learner will be able to

a) Operate AI software tools for generative cybersecurity measures
b) Assemble AI-driven cybersecurity solutions using cloud platforms
c) Use AI frameworks and libraries to enhance cybersecurity protocols

⭡ Back to the Programme Structure

Business Resilience and Response Strategies
Compulsory
6 ECTS
Term 2

Course Description

This course emphasizes the importance of business resilience in the face of cybersecurity threats. It covers strategies to ensure business continuity, disaster recovery, and effective response to security breaches, equipping students with the knowledge to mitigate risks and ensure business operations.

Tentative list of topics:

- Fundamentals of Business Resilience
- Business Continuity and Disaster Recovery Planning
- Incident Response Management
- Crisis Communication and Stakeholder Management
- Case Studies: Handling Major Cybersecurity Incidents

Applying Knowledge and Understanding

At the end of the module/unit the learner will have acquired the following skills:

a) Design robust business continuity and recovery plans
b) Analyze incident reports to strategize effective responses
c) Communicate effectively during cybersecurity crises

Module-Specific Learner Skills

At the end of the module/unit the learner will be able to

a) Design robust business continuity plans tailored to cyber threats
b) Apply crisis communication strategies during cybersecurity incidents
c) Demonstrate the ability to recover from cybersecurity breaches

Module-Specific Digital Skills and Competences

At the end of the module/unit, the learner will be able to

a) Use digital tools to simulate and test business resilience strategies
b) Operate incident response platforms to manage cybersecurity crises
c) Assemble digital dashboards to monitor business continuity in the face of cyber threats

🠝 Back to the Programme Structure

Behavioral Cybersecurity
Elective
6 ECTS
Term 2

Course Description

Delving into the human aspect of cybersecurity, this course explores the behavioral patterns that contribute to security vulnerabilities. It emphasizes understanding human psychology, fostering a security-conscious culture, and strategies to mitigate human-related risks.

Tentative list of topics:

- Introduction to Behavioral Cybersecurity
- Psychological Aspects of Security Vulnerabilities
- Training and Awareness Programs
- Social Engineering Attacks and Countermeasures
- Case Studies: Human-driven Security Breaches

Applying Knowledge and Understanding

At the end of the modules/units the learner will have acquired the following skills:

a) Analyze human-driven security incidents
b) Design training and awareness programs to enhance security behavior.
c) Implement measures to counteract social engineering attacks

Module-Specific Learner Skills

At the end of the modules/units the learner will be able to

a) Apply psychological principles to counteract social engineering attacks
b) Design training programs focused on improving cybersecurity behavior
c) Demonstrate an understanding of human-driven vulnerabilities in cyber contexts

Module-Specific Digital Skills and Competences

At the end of the modules/units, the learner will be able to

a) Use digital platforms to disseminate cybersecurity awareness content
b) Operate behavioral analysis tools to detect human-centric vulnerabilities
c) Create digital simulations to test human responses to cyber threats

⬆ Back to the Programme Structure

Cloud and IoT Security

Elective
6 ECTS
Term 2

Course Description

This course focuses on the security challenges and solutions specific to cloud computing and the Internet of Things (IoT). It covers techniques to ensure data integrity, privacy, and compliance in cloud and IoT environments.

Tentative list of topics:

- Introduction to Cloud Security
- IoT Security Challenges and Solutions
- Data Protection and Privacy in the Cloud
- Security Protocols for IoT Devices
- Case Studies: Cloud and IoT Security Incidents

Applying Knowledge and Understanding

At the end of the module/unit the learner will have acquired the following skills:

a) Design secure cloud architectures and IoT device configurations
b) Analyze vulnerabilities in cloud services and IoT networks
c) Implement security protocols tailored for cloud and IoT environments

Module-Specific Learner Skills

At the end of the module/unit the learner will be able to

a) Design security protocols tailored for cloud and IoT environments
b) Apply best practices to ensure secure data storage and transit in the cloud
c) Demonstrate an understanding of the unique challenges posed by IoT device security

Module-Specific Digital Skills and Competences

At the end of the module/unit, the learner will be able to

a) Use cloud platforms to configure and monitor security settings
b) Operate IoT device management tools to ensure secure connectivity
c) Assemble secure cloud architectures using industry-standard tools

⭡ Back to the Programme Structure

Secure Software Development

Elective
6 ECTS
Term 2

Course Description

This course introduces students to the best practices in developing secure software. It emphasizes the software development lifecycle's security aspects, from design to deployment, ensuring that software is resilient to threats.

Tentative list of topics:

- Secure Coding Practices
- Threat Modeling in Software Design
- Security Testing and Validation
- Patch Management and Vulnerability Handling
- Case Studies: Software Vulnerabilities and Exploits

Applying Knowledge and Understanding

At the end of the module/unit the learner will have acquired the following skills:

a) Implement secure coding practices across various programming languages
b) Analyze software for vulnerabilities and potential threats
c) Design software solutions with security as a core principle

Module-Specific Learner Skills

At the end of the module/unit the learner will be able to

a) Design software solutions with security as a foundational principle
b) Apply secure coding practices across a range of programming languages
c) Demonstrate the ability to test and patch software vulnerabilities

Module-Specific Digital Skills and Competences

At the end of the module/unit, the learner will be able to

a) Use integrated development environments (IDEs) with security plugins
b) Operate software vulnerability assessment tools
c) Create and manage a secure software deployment pipeline

↑ Back to the Programme Structure

Critical Thinking and Problem-Solving

Elective

6 ECTS

Term 2

Course Description

This course nurtures the analytical skills required in cybersecurity roles. It emphasizes the ability to critically assess security challenges, develop mitigation strategies, and solve complex cybersecurity problems.

Tentative list of topics:

- Introduction to Critical Thinking in Cybersecurity
- Analytical Problem-Solving Techniques
- Scenario-Based Security Challenges
- Risk Assessment and Mitigation
- Case Studies: Complex Security Problem Solving

Applying Knowledge and Understanding

At the end of the module/unit the learner will have acquired the following skills:

a) Apply critical thinking techniques to real-world cybersecurity scenarios

b) Design strategies for effective problem-solving in cyber incidents

c) Evaluate cybersecurity solutions with a critical mindset

Module-Specific Learner Skills

At the end of the module/unit the learner will be able to

a) Apply structured problem-solving techniques to cyber challenges

b) Design strategies to effectively handle complex cybersecurity incidents

c) Demonstrate the ability to evaluate cyber solutions critically

Module-Specific Digital Skills and Competences

At the end of the module/unit, the learner will be able to

a) Use digital platforms for brainstorming and strategy sessions

b) Operate cybersecurity tools with a critical mindset to detect false positives

c) Arrange digital data in a way that facilitates critical analysis

⬆ Back to the Programme Structure

Leadership & Communication in Cybersecurity

Elective

6 ECTS

Term 2

Course Description

This course delves into the leadership and communication skills essential for cybersecurity professionals. It emphasizes the importance of effectively communicating security concerns, strategies, and solutions to both technical and non-technical stakeholders.

Tentative list of topics:

- Leadership in Cybersecurity
- Effective Communication Strategies
- Stakeholder Engagement and Management
- Crisis Communication in Security Incidents
- Case Studies: Leading Security Initiatives

Applying Knowledge and Understanding

At the end of the module/unit the learner will have acquired the following skills:

a) Lead cybersecurity teams with effective decision-making and delegation
b) Communicate complex cybersecurity topics to varied audiences
c) Design strategies for effective internal and external cybersecurity communications

Module-Specific Learner Skills

At the end of the module/unit the learner will be able to

a) Design communication strategies tailored for cybersecurity audiences
b) Apply leadership principles in the context of cybersecurity teams
c) Demonstrate effective delegation and decision-making in cyber operations

Module-Specific Digital Skills and Competences

At the end of the module/unit, the learner will be able to

a) Use digital platforms for effective team communication and collaboration
b) Operate cybersecurity dashboards to communicate effectively with stakeholders
c) Arrange digital cybersecurity presentations for diverse audiences

⭡ Back to the Programme Structure

AI-Driven Forensic Analysis in Cybersecurity

Elective

6 ECTS

Term 2

Course Description

This course focuses on the application of AI in cyber forensic analysis. It covers techniques to utilize AI-driven tools for faster and more accurate forensic investigations after security incidents.

Tentative list of topics:

- Introduction to Cyber Forensics
- AI in Forensic Data Analysis
- Automated Forensic Toolkits
- AI-Driven Incident Analysis
- Case Studies: AI in High-profile Forensic Investigations

Applying Knowledge and Understanding

At the end of the module/unit the learner will have acquired the following skills:

a) Apply AI-driven techniques in forensic investigations
b) Design AI-enhanced forensic strategies for cyber incidents
c) Use AI tools and frameworks tailored for cyber forensic analysis

Module-Specific Learner Skills

At the end of the module/unit the learner will be able to

a) Design forensic analysis strategies leveraging the power of AI
b) Apply AI-driven techniques to extract insights from cyber incidents
c) Demonstrate an understanding of integrating AI with traditional forensic methodologies

Module-Specific Digital Skills and Competences

At the end of the module/unit, the learner will be able to

a) Use AI platforms tailored for cyber forensic analysis
b) Operate tools and frameworks that combine AI and cyber forensics
c) Arrange and present AI-driven forensic findings in a coherent and interpretable manner

⬆ Back to the Programme Structure

Capstone Project and Dissertation - for students completing MSc at 90 ECTS
Compulsory
30 ECTS
Term 3

Course Description

The Capstone Project and Dissertation is the most significant project assigned to students throughout their program. It is intended to consolidate the skills gained during the program through a research project. Each student, together with an OPIT supervisor, will work on a project proposal that will then be realized through the final terms of their program. The project needs to be a research work of industrial relevance that investigates methodological and/or practical aspects in any of the domains discussed in the program and beyond. Students will also have the opportunity to conduct internships with industrial partners as a way to work and complete their Capstone Project and Dissertation module. In general, the dissertation document should show that the student has achieved mastery of the field and is fully conversant with the relevant literature.

The capstone project is the longest and most challenging project assigned to a student, requiring a long preparation and hard work. The supervisor's role is to guide the student since most of the project should be carried on as an independent work. Students are required to prepare a document where they will describe the project goals and the obtained results. The results should provide enough depth within a particular field of application and be consistent with the original plan agreed with the supervisor. At the end of the process, the student would have learnt to conduct independent research, problem-solving, numerical mastery, project management, time management, and self-discipline, amongst others.

The thesis will be presented to an examining committee. The student will be expected to defend the work done and the results presented. This happens typically via an oral examination called a viva, where the student presents their work and answers questions from the committee.

The final thesis manuscript should consist of 10,000 - 20,000 words.

Applying Knowledge and Understanding

At the end of the module/unit the learner will have acquired the following skills:

a) Apply research methodologies to explore, analyze, and address complex cybersecurity challenges
b) Practice structured writing techniques to produce a comprehensive research document
c) Demonstrate a deep understanding of a chosen cybersecurity topic, substantiating claims with evidence
d) Show the ability to critically review existing literature and identify gaps or areas of improvement
e) Plan and execute a research project within a stipulated time-frame, ensuring milestones are met
f) Design experiments or simulations, as applicable, to validate hypotheses or research questions

g) Operate relevant cybersecurity tools and platforms to gather, analyze, and present data
h) Assemble and organize research findings in a coherent and logical manner, ensuring a flow of ideas
i) Use feedback from peers and advisors to refine and improve the research process and outcomes
j) Construct arguments and discussions backed by empirical evidence or theoretical frameworks
k) Prepare and present findings to both technical and non-technical audiences, ensuring clarity and understanding
l) Create actionable recommendations or solutions based on research findings, ensuring they are practical and implementable
m) Compose a comprehensive document that adheres to academic standards and is free from plagiarism
n) Arrange findings, discussions, and conclusions in a structured manner, ensuring the document is reader-friendly and organized

Module-Specific Learner Skills

At the end of the module/unit the learner will be able to

a) Manage their own learning process, setting research goals, and milestones in line with the project's objectives
b) Negotiate with potential stakeholders, if applicable, to gather necessary data or insights for the research
c) Supervise and ensure the ethical collection and use of data, respecting privacy and confidentiality standards
d) Guide discussions and arguments in the research, ensuring they are grounded in evidence and sound reasoning
e) Authorize and finalize the submission of the research, ensuring all academic and institutional criteria are met

Module-Specific Digital Skills and Competences

At the end of the module/unit, the learner will be able to

a) Operate specialized software or platforms relevant to the research topic, ensuring accurate data collection and analysis
b) UtilizeUtilise digital tools for literature review, citation management, and plagiarism checking
c) Arrange and visualize data using appropriate digital tools, ensuring clear representation of findings
d) Design and run simulations or models, if applicable, to validate hypotheses using dedicated software
e) Apply cybersecurity tools to protect research data, ensuring its integrity and confidentiality
f) Compose the research document using digital word processing software, adhering to specified formatting standards

⬆ Back to the Programme Structure

Capstone Project and Dissertation - for students completing MSc at 120 ECTS

Compulsory

60 ECTS

Term 3 - 4

Course Description

The Capstone Project and Dissertation is the most significant project assigned to students throughout their program. It is intended to consolidate the skills gained during the program through a research project. Each student, together with an OPIT supervisor, will work on a project proposal that will then be realized through the final terms of their program. The project needs to be a research work of industrial relevance that investigates methodological and/or practical aspects in any of the domains discussed in the program and beyond. Students will also have the opportunity to conduct internships with industrial partners as a way to work and complete their Capstone Project and Dissertation module. In general, the dissertation document should show that the student has achieved mastery of the field and is fully conversant with the relevant literature.

The capstone project is the longest and most challenging project assigned to a student, requiring a long preparation and hard work. The supervisor's role is to guide the student since most of the project should be carried on as an independent work. Students are required to prepare a document where they will describe the project goals and the obtained results. The results should provide enough depth within a particular field of application and be consistent with the original plan agreed with the supervisor. At the end of the process, the student would have learnt to conduct independent research, problem-solving, numerical mastery, project management, time management, and self-discipline, amongst others.

The thesis will be presented to an examining committee. The student will be expected to defend the work done and the results presented. This happens typically via an oral examination called a viva, where the student presents their work and answers questions from the committee.

The final thesis manuscript should consist of 150,000 - 30,000 words.

The module instance described here is worth 60 ECTS. The main differences between a 30 and a 60 ECTS Capstone Project and Dissertation are the duration and the value of the results reached by the students. Students opting for the 60 ECTS version will be required to work two full Terms (instead of one) on the module and will be expected to produce results that are publishable in relevant journals and/or conference proceedings. On the other hand, students working on the 30 ECTS version are not expected to reach that level of quality at the time of graduation.

Applying Knowledge and Understanding

At the end of the module/unit the learner will have acquired the following skills:

a) Apply research methodologies to explore, analyze, and address complex cybersecurity challenges
b) Practice structured writing techniques to produce a comprehensive research document
c) Demonstrate a deep understanding of a chosen cybersecurity topic, substantiating claims with evidence
d) Show the ability to critically review existing literature and identify gaps or areas of improvement
e) Plan and execute a research project within a stipulated time-frame, ensuring milestones are met
f) Design experiments or simulations, as applicable, to validate hypotheses or research questions
g) Operate relevant cybersecurity tools and platforms to gather, analyze, and present data
h) Assemble and organize research findings in a coherent and logical manner, ensuring a flow of ideas
i) Use feedback from peers and advisors to refine and improve the research process and outcomes
j) Construct arguments and discussions backed by empirical evidence or theoretical frameworks
k) Prepare and present findings to both technical and non-technical audiences, ensuring clarity and understanding
l) Create actionable recommendations or solutions based on research findings, ensuring they are practical and implementable
m) Compose a comprehensive document that adheres to academic standards and is free from plagiarism
n) Arrange findings, discussions, and conclusions in a structured manner, ensuring the document is reader-friendly and organized

Module-Specific Learner Skills

At the end of the module/unit the learner will be able to

a) Manage their own learning process, setting research goals, and milestones in line with the project's objectives
b) Negotiate with potential stakeholders, if applicable, to gather necessary data or insights for the research
c) Supervise and ensure the ethical collection and use of data, respecting privacy and confidentiality standards
d) Guide discussions and arguments in the research, ensuring they are grounded in evidence and sound reasoning
e) Authorize and finalize the submission of the research, ensuring all academic and institutional criteria are met

Module-Specific Digital Skills and Competences

At the end of the module/unit, the learner will be able to

a) Operate specialized software or platforms relevant to the research topic, ensuring accurate data collection and analysis

b) UtilizeUtilise digital tools for literature review, citation management, and plagiarism checking

c) Arrange and visualize data using appropriate digital tools, ensuring clear representation of findings

d) Design and run simulations or models, if applicable, to validate hypotheses using dedicated software

e) Apply cybersecurity tools to protect research data, ensuring its integrity and confidentiality

f) Compose the research document using digital word processing software, adhering to specified formatting standards

⬆ Back to the Programme Structure