

IB9HG-15 Cybersecurity in Finance

27/28

Department

Warwick Business School

Level

Taught Postgraduate Level

Module leader

Kalina Staykova

Credit value

15

Module duration

10 weeks

Assessment

20% coursework, 80% exam

Study location

University of Warwick main campus, Coventry

Description

Introductory description

This module introduces key cybersecurity issues in the financial sector, focusing on the technologies, threats, risks, and governance challenges that affect modern banking, fintech, payment systems, and digital financial ecosystems. The module combines foundational cybersecurity principles and concepts such as cyber risk and controls with practical financial applications, including data protection, fraud prevention, cloud and API security, blockchain security, operational resilience, and regulatory compliance. Through case studies, simulations, and strategic analysis, students will develop the ability to identify cyber threats and required security controls, evaluate security frameworks, and understand how cybersecurity supports trust, stability, and innovation in digital finance. The purpose of the module is not to train students to become cyber technology experts, but to teach students, who are to perform various organizational roles (also within cybersecurity), to be aware of and know how to address diverse cyber security issues in digital finance.

[Module web page](#)

Module aims

The module introduces students to the fundamental principles, concepts, and practices of cybersecurity within the context of the financial services industry. It provides in-depth

understanding of various cyber-attacks affecting banks, fintech companies, payment systems, digital platforms, and financial infrastructures, the motivations behind them, the processes through which these attacks unfold and the responses, which an organization can adopt to defend itself.

The module also provides insights into how financial organizations of various sizes (e.g., established financial institutions and FinTech start-ups) can effectively build and implement a cybersecurity program, which includes aspects such as the identification of relevant cyber risks, building appropriate technology and procedural controls, and raising awareness among relevant stakeholders (employees, users, suppliers) by promoting dedicated cyber culture and providing ongoing training. We also introduce emerging cybersecurity challenges associated with cloud computing, open banking, APIs, artificial intelligence, blockchain, and fintech platformization and outline approaches how to address them.

The module deals with topics such as cyber-attack types in digital finance, attacks anatomy, (active) cyber defence (controls), incident response management, blockchain security, fraud (AI fraud analytics), data security, security models (perimeter-based security model, zero-trust, defence-in-depth, cloud native security model, API security model, identity-centric security models, risk-based security models, DevSecOps Security Model, AI-Driven Security Model).

While this is not a technical module, we will provide sufficient understanding of important technical aspects of cybersecurity such as backup recovery, intrusion detection, system monitoring, penetration testing, the use of AI and ML in cyber defence, security-by-design, firewalls, patch management, cryptography, identity and access management, etc.

Throughout the module, we will delve into some of the most prominent cyber-attack cases in digital finance and work with established cybersecurity frameworks, standards, and methodologies.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

Whilst the module teaching is not a technical cyber security coding course, it will cover a wide range of subject matter knowledge in this space which is essential to understand the risks and threats of technology. It will also consider social and psychological behavior techniques as well. This will exceed the general cyber security certifications available and use applied business strategy theory with cyber security knowledge in a business context.

We relate the module to leading InfoSec certifications CompTIA Security+, GSEC SANS GIAC Security Essentials, including CISSP Certified Information Systems Security Professional, CEH certified ethical hacker, ECSA - EC-Council Certified Security Analyst, CISM Certified Information Security Manager, ISACA Certified Information Security Auditor CISA, (ISC)² Certified Cloud Security Professional CCSP, CRISC Certified in Risk and Information Systems Control. GCHQ Certified Training (GCT)

This module is not part of the GCHQ Degree Certification, or the NCSC certification program.

Learning outcomes

By the end of the module, students should be able to:

- Demonstrate in-depth knowledge of and ability to critically evaluate key cybersecurity concepts (e.g., organizational and security controls, defence in depth, vulnerabilities, incident response, situational awareness, cybersecurity awareness and training), frameworks and standards (e.g., NIST) and theories (e.g., deterrence theory).
- Demonstrate understanding of current and emerging cyber security issues in digital finance, trends and research from a business a management perspective
- Demonstrate comprehensive understanding and ability to outline a complete anatomy of a significant FinTech security incident from initial compromise through impact, response, and recovery, identifying the governance implications at each stage
- Identify, analyze and outline the principal technical and operational security controls relevant to financial organizations in terms accessible to a non-technical commercial audience, explaining the purpose, limitations, and equity implications of each
- Demonstrate critical situation analysis from a cybersecurity view
- Demonstrate creativity in determining cyber-attacks and required defences
- Demonstrate thinking skills in anticipating moves and counter moves of threat agents, and the cost and effectiveness of these counter moves

Indicative reading list

[Reading lists can be found in Talis](#)

Interdisciplinary

The module explores cybersecurity from socio-technical perspective. We also explore regulatory and societal issues related to cybersecurity.

Subject specific skills

Design, implement and assess a comprehensive cybersecurity program for a financial organization (including incident response plan, business continuity plan).

Design and evaluate security controls for a financial organization.

Exhibit ability to perform key analyses (e.g., threat and risk assessments; identify mid-term and long-term impacts of cyber-attacks on financial organizations and strategies for mitigating these impacts; apply key cybersecurity frameworks and principles) and critically evaluate findings

Identify and classify the principal cybersecurity threats facing FinTech organisations by actor, motivation, method, and target

Transferable skills

Analytical skills

Critical thinking skills

Written skills

Study

Study time

Type	Required
Lectures	9 sessions of 1 hour (6%)
Other activity	18 hours (12%)
Private study	51 hours (34%)
Assessment	72 hours (48%)
Total	150 hours

Private study description

Private study to include preparation for lectures/ seminars/ workshops and own reading

Other activity description

9 x 2 hrs workshops

Costs

No further costs have been identified for this module.

Assessment

You do not need to pass all assessment components to pass the module.

Assessment group D1

	Weighting	Study time	Eligible for self-certification
Assessment component			
Group Presentation Slides	20%	14 hours	No
Group presentation slides - 16 slides maximum			
Reassessment component			
Individual assignment			Yes (extension)

	Weighting	Study time	Eligible for self-certification
--	-----------	------------	---------------------------------

Assessment component			
----------------------	--	--	--

2 hr written exam	80%	58 hours	No
-------------------	-----	----------	----

- Answerbook Pink (12 page)

Reassessment component is the same

Feedback on assessment

Feedback via My.WBS

[Past exam papers for IB9HG](#)

Availability

Courses

This module is Core for:

- Year 1 of TIBS-H60Z MSc Financial Technology