IB9HG-15 Cybersecurity in Business

26/27

Department
Warwick Business School
Level
Taught Postgraduate Level
Module leader
Kalina Staykova
Credit value
15
Module duration
10 weeks
Assessment
100% coursework
Study location
University of Warwick main campus, Coventry

Description

Introductory description

This module introduces cybersecurity within a broader business context. It seeks to outline how various types of organizations (e.g., start-ups, SMEs, and large multinational organizations; public and private; digital natives vs non-digital natives, etc.) design and implement cybersecurity programs in order to protect their digital technologies, data and information systems (IS), and other business assets from a myriad of cyber threats. To this end, we investigate cybersecurity issues from organizational, strategic, behavioural, technical, and regulatory perspectives. 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 various cyber security (as well as privacy) issues in strategic IS context.

Module web page

Module aims

The module explores the role of people, processes, and technology in cybersecurity. It provides in-depth understanding of various cyber attacks, 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 an organization 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 will also investigate issues related to the alignment of the cybersecurity program with an organisation's business strategy, employee compliance to an organization's cybersecurity program as well as the program's compliance to existing regulation.
The module deals with topics such as cyber attack types, attacks anatomy, (active) cyber defence (controls), incident response management, cyber organizational readiness and cyber resilience, cyber risk and threat intelligence, cyber insurance, cyber awareness and training, and cyber regulation. 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 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, SANS) and theories (e.g., deterrence theory).
- Demonstrate comprehensive understanding and ability to outline the role and responsibilities of the Chief Information Security Officer (CISO), the cybersecurity team and their interplay with the rest of the organization as well as with external stakeholders (regulators, partners, users, etc.).

- Demonstrate understanding of current and emerging cyber security issues, trends and research from a business a management perspective.
- Demonstrate critical situation analysis in businesses and organizations from a cybersecurity view
- Demonstrate creativity in determining cyber attacks and required defences
- Demonstrate thinking skills in anticipating moves and counter moves of enemies, and the cost and outcome risks

Indicative reading list

Reading lists can be found in Talis

Interdisciplinary

The module explores cyber security and attacks from different perspectives of hackers, criminal, political, industrial and regulatory perspectives.

Subject specific skills

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

Design and evaluate organizational and security controls.

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

Transferable skills

Written skills.

Teamwork.

Study

Study time

Type	Required
Lectures	10 sessions of 1 hour (7%)
Other activity	20 hours (13%)
Private study	48 hours (32%)
Total	150 hours

Type	Required
Assessment	72 hours (48%)
Total	150 hours

Private study description

Self study to include pre-reading for lectures

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 A5

	Weighting	Study time	Eligible for self-certification
Assessment component			
Group Presentation Slides 16 slides maximum	20%	14 hours	No
Reassessment component			
Individual assignment			Yes (extension)
Assessment component			
Individual assignment	80%	58 hours	Yes (extension)
Reassessment component is the same			

Feedback on assessment

Feedback via My.WBS

Availability

Courses

This module is Core for:

- Year 1 of TIBS-G5N4 Postgraduate Taught Management of Information Systems and Digital Innovation