# Cyber security regulation

## Proff. Daniele Frasca; Federico Panisi

***COURSE AIMS AND INTENDED LEARNING OUTCOMES***

The course aims to provide students with an understanding of the principles underlying the legislation regarding cybersecurity in force in the European Union. While focusing on cybersecurity regulation, the course will teach what problems arise in the context of cybersecurity and what economic rationales justify its regulation. Moreover, the class intends to offer an overview of the best practices that complex economic agents employ to make their activity comply with the cybersecurity regulation in force. At the end of the course, students will be able to understand the core principle of EU cybersecurity regulation and navigate through their more relevant complexities from a theoretical and practical standpoint. The class will be structured based on two modules. The lecturer of the first module - a lawyer with broad international experience and a Stanford University graduate - will provide students with the theoretical foundations. Throughout the second module, the partner of one of the most prestigious international consultancy firms will guide students through the process of building cybersecurity measurement models. The class will have a unique ‘hands-on’ approach and conclude with students presenting their project works. The course does not have prerequisites, and due to the nature of the class, students are highly encouraged to attend it.

***MODULE I: Prof. Federico Panisi***

***COURSE CONTENT***

● **Introduction**

Context & background:

a. data as the new oil of the Internet and the new currency of the digital World.

b. An interesting case study for the regulation of cybersecurity regulation: operation *Aurora*.

What is cybersecurity, and why it is important.

● **The economics of cybersecurity**

The insufficiency of ordinary remedial means before cybersecurity breaches.

The occurrence of market failures in relation to cybersecurity provision:

a. negative externalities and overproduction of cyber *in*security.

b. Cybersecurity as a public good. Positive externalities and the underproduction of cybersecurity.

c. Cybersecurity from the eyes of the ‘Tragedy of the commons.’

The long walk towards a (socially) optimal level of cybersecurity. Private

 *vs* public ordering.

● **Cybersecurity regulation**

The European Union (EU) strategic initiatives in relation to cybersecurity:

a. the EU cybersecurity strategy.

b. The Digital Single Market strategy.

The EU cybersecurity regulation:

a. ENISA’s Regulation.

b. NIS Directive.

c. GDPR.

d. DORA.

***MODULE II: Prof. Daniele Frasca***

***COURSE CONTENT***

* **Cybersecurity regulatory frameworks in action: which principles and requirements mainly impact complex organizations?**

Understanding the main cyber risks and challenges and the impact of the main principles and requirements of the European Cybersecurity regulation:

a. Cyber risks

b. Cyber Regulation

o NIS

o DORA

o General Data Protection Regulation (GDPR);

o International Standards: ISO, NIST, ENISA guidelines

* **Operational best practices for the Cybersecurity of complex organizations**

Understanding the industry's best practices to ensure adherence to the EU Cybersecurity regulation according to an end-to-end approach (identify, protect, detect, protect, respond, recover, learn & improve):

a. Situational Awareness (e. g. identification of critical processes and interdependencies) & Threat Intelligence

b. Cyber Risk Management and its evolution

c. Security controls, testing, and measurement of digital operational resilience levels

* **Addressing cyber challenges through solutions and technologies**

Understanding how managers and companies are addressing the problem of complying with the EU Cybersecurity regulation:

a. Automation and Governance, Risk, and Compliance (GRC) tools and software

b. AI & Cloud computing solutions supporting data security, data analysis, and data governance

c. ICT Process optimization and IT Project management.

* **The future challenges of technology regulation**: the Trustworthy AI regulation & framework

***READING LIST***

During the lessons, the lecturers will provide papers, documents, and other reading material relevant to the course produced by international public or private institutions or university research centers, or other international research fora.

***TEACHING METHOD***

In-class lectures. During the lecturing of Module II, company representatives, and managers will be involved within the class to present use cases related to the course program.

***ASSESSMENT METHOD AND CRITERIA***

Students are invited to produce and present a final project work. The project aims to build an organization’s cyber resilience measurement model (1. Situational Awareness; 2. Security controls framework; 3. Risk assessment methodology; 4. Testing). Specifically, each team will have to focus on a section of the overall process to achieve the measurement model. Students’ project works will be evaluated mostly upon (1) the coherence between the objectives achieved and the ultimate goal of the class (building a cyber resilience measurement model), (2) the coherence between the objectives declared for each project work and the methodologies employed to achieve them, and (3) the abilities to communicate the results to the class effectively. In any case, the teachers will provide students with further information about it at the very beginning of the course.

***NOTES AND PREREQUISITES***

*Warning and prerequisites*

Because the module is an introduction to cybersecurity, attending the class does not have prerequisites for content.

*Time and Place to meet students*

Students are invited to meet with the lecturers throughout the whole course.

The office time will take place at the time and in the room of Università Cattolica del Sacro Cuore, Brescia, which each lecturer is communicating on the first day of classes.