Teamwork
How to improve organizational aspects of cybersecurity

Organizational Sciences Module

Professor Federico Niccolini – Dottoressa Martina Neri

1

Teaching methods and assessment

	Teamwork	Final examination
Number of components	4	1
Weight	**35%**	65%
Object	1 case study autonomously selected by each group	Program
Evaluation	The vote obtained will be weighted according to the percentage specified above	

Method of examination

Written and oral

Only oral if Assessment$_{TW}\geq$ 30

2

1

Teaching methods and assessment

- Enhance students' **knowledge, analytical skills** about the principles, theories, and methodologies of organizational sciences within cybersecurity related issues

- **In-depth analysis of organizational perspectives in the cybersecurity field** and increasing interpretive skills with up-to-date and influential material

- **Practical application** of organizational perspectives within cybersecurity

- Improving the **soft skills** of **learning by interacting, and public speaking, and problem solving** thanks to the **participatory approach**

3

Team work

Scope and Objectives

- Analyze through the lens of the **principles of cyber organizational sciences** a real case study

- Develop **critical thinking** toward organizational cyber issues

- Interpret the case study and **propose possible organizational solutions**

- Develop a plan to **improve the organization's cybersecurity**

4

GUIDELINES

1) **Team forming** – create a groups of 3/4 people

2) Case study selection

3) Team work **main phases**:

Phase 1: Case study framework: analysis taking into account: 1) sector; 2) size (micro, small, medium, or large) according to European Commission guidelines; 3) main business activity (type of product or service, target customer)

Phase 2: Case study contingent analysis: examination of the current cybersecurity situation/posture

Phase 3: Planning: according to the previous analysis you will act as a cybersecurity manager, thus proposing a plan to improve the organizational cybersecurity

5

GUIDELINES

4) Elaboration and **presentation**: Max 20 mins of presentation and 10 mins discussion

5) **Constructive criticism by peers**: teams not presenting will follow the presentations and have to identify and expose at least one strength and one point of improvement of of the presentation

6) Each team will receive an evaluation based on the quality of **both** the work presented and the criticism produced

7) A list of **mandatory and optional topics** to be applied to the analysis will be provided to each team. You must choose **3 topics (2 mandatory and 1 optional).** For each topic chosen, you must identify **both** the existing/actual situation and make a proposal to enhance it in the plan.

6

MANDATORY TOPICS

1)   Strategy

1.1   SWOT analysis

1.2   Operative goals for cybersecurity

2)   Cyber organizational culture

2.1 Organizational mechanism regarding cybersecurity culture

2.1.1 Communication channels

2.1.2 Training

2.1.3 Organizational learning mechanisms

2.1.4 Artefacts used to create a cybersecurity culture

3)   Organizational resilience (including the cyber one)

3.1 Tools and practices for anticipation

3.1.1 Training

3.1.2 Plans implementation

3.2 Tools and practices for withstanding and coping

3.2.1 Cybersecurity expert role

3.3 Tools and practices for recovery and learning

3.3.1 Learning mechanism

3.3.2 Feedback analysis

4)   Organizational structure

4.1   Structural designs for organizational cybersecurity (e.g., functional structure over divisional)

4.2   Strengths and weaknesses of the structural design

4.3   Information-sharing design (e.g., vertical vs horizontal)

OPTIONAL TOPICS (examples)

1)   Cybersecurity awareness

1.1   Education plans

2) Strategic alliances and other partnerships

3) ....

EXAMPLES

1.1/2 SWOT analysis and strategy: A) Do the SWOT analysis of the actual organizational cybersecurity of the case study; **B)** Propose solutions to the identified weakness; **C)** Propose strategies and activities on how to counteract threats; **D)** Propose strategies and activities on how to exploit opportunities.

4.1. Structural designs: A) identify the structural design of your case study; **B)** Depict its features (e.g., is there a cybersecurity function? Which is the information sharing design?); **C)** propose changes to the structural design to enhance organizational cybersecurity.

9

Presentation guidelines

- **Time** → Max 20 minutes

- **Contents** → The presentation must be developed as follows:

- **First slide:** Title and table of contents

- **Second and third slides:**

Case study framework → 1) sector; 2) size (micro, small, medium, or large) according to European Commission guidelines; 3) main business activity (type of product or service, target customer)

- **Fourth to eight slides:**

Current organizational cybersecurity situation

- **Nineth and subsequent slides :**

Organizational cybersecurity plan

10

Presentation guidelines

- **Citations:** At the end of each presentation, it is required to provide a **clear specification of the topics selected** for the case study analysis (you must refer either to the books, articles, and slides). Thus, a bibliography must be presented at the end.

- **Overall requirements:** Please note that students are required to participate in all the phases of the teamwork.

11

Team forming

Group	Names	Case study
TW1	Fabio Chiarini, Giovanni D'Ambrosio, Stefano Hidalgo, Sergio Zambelli	Valve Corporation https://www.valvesoftware.com/it/
TW2	Giovanni Cisternini, Chiara Gualtieri, Umberto Melpignano, Federico Rossetti	Reply – www.reply.com
TW3	Niccolò Brandolini, Hatem Elashmawy, Gregorio Manduzio, Massimiliano Mattei	UniPi
TW4	Diego Bernardini, Giuseppe Conte, Leonardo Corsini, Lemi Oliver	Cellbrite – https://cellbrite.com

12