הפקולטה לניהול ע"ש קולר אוניברסיטת תל אביב

Coller School of Management Tel Aviv University

בית הספר למוסמכים במינהל עסקים ע"ש ליאון רקנאטי

# Organization Preparation for Cybersecurity Threats

## 1242.3278.01

Course Prerequisites: None

| | |
|---|---|
| **Term** | Fall 2021 / Second half |
| **Day** | Sunday |
| **Hour** | 18:45 – 21:30 |
| **Room** | 303 |
| **Final Exam** | The students will have a final-project to submit |
| **Lecturer** | Dr. Jacob Mendel |
| **Email** | jacob4x4@gmail.com |
| **Telephone** | 054-4547369 |
| **Office** | 445 |
| **Language** | English / Hebrew |
| **Teaching Assistant (TA)** | Dr. Rafael Hod, rhod@tau.ac.il |

Office Hours: By appointment

## Course Units

**Course Units: 1 CU**

4 ECTS (European Credit Transfer and Accumulation System) = 1 course unit.

By making higher education comparable across Europe, ECTS makes teaching and learning in higher education more transparent and facilitates the recognition of all studies.

## Objectives

Upon course completion, students will develop a clear understanding of cybersecurity attacks and their economic impact on different industries use cases. The students will acquire a range of skills allowing them to assess and practice effectively in different fields.

- Understanding the economic impact of cyber attacks
- Business challenges and problems when preparing organization to cyber attacks
- Better understanding of business needs and the connection cybersecurity
- Evaluate cyber-attacks and their economic impact
- Understand how cybersecurity is applied to different aspects of the business and how to overcome different barriers
- Expose the students to cybersecurity risk management

## Course Description

### Cyber Threats of Tomorrow: How Should You Prepare Your Organization

Cyber-attacks and their complexity are increasing at a high rate. Each organization must take into account that it will be very difficult to identify and stop some of the cyber-attacks. Organization must prepare for its continued operations while cyber-attack on it. The focus of organizations solely on the prevention of cyber-attacks by investing in improving defense capabilities and adopting new technologies is nowhere near enough. Organizations must prepare for cyber events while improving their response capabilities and recovery mechanisms. Failure to prepare the organization and a tentative or incorrect response can put the organization in a very dangerous business and legal situation. However, many organizations refrain from preparing themselves for managing and recovering from cyber events, preferring to leave the issue to the care and responsibility of the organization's infrastructure and computing manager. The purpose of the session is to learn and experience complex events, understanding the tools and technologies for dealing with business questions and challenges in the digital age.

Cyber-attacks and their complexity are increasing at a high rate. Every organization must take into account that it will be very difficult to identify and stop some of the cyber-attacks, which means that the organization must prepare for business continuation while a cyber-attack is ongoing. Organizations' focus solely on preventing cyber-attacks by investing in improving defense capabilities and adopting new technologies is not sufficient at all today. Organizations need to prepare for cyber events while improving their response capabilities and recovery mechanisms. Non-preparation of the organization and a hesitant response or incorrect response, can put the organization in a very dangerous business and legal situation. However, many organizations refrain from preparing themselves for managing and recovering from cyber incidents, preferring to leave the issue to the care and responsibility of the organization's infrastructure and computing manager. Some cyber incidents are characterized, among other things, by sophisticated and innovative methods of attack, which sometimes originate from external parties that provide various services to organizations. These factors are included in the supply chain (Supply Chain) of the organizations.

Building a cyber crisis management plan that describes the responsibilities and actions required between all relevant parties, i.e., the technological teams (research and development, network, communications, applications, information security, etc.), senior executives, risk managers, legal advisers, public relations and spokespersons, crisis management consultants and more. Proper cooperation between the above factors is critical to the organization's ability to act correctly at the time of the event which is characterized by great uncertainty. The plan should provide clear ways to manage the event, as it addresses the unique requirements of the organization, takes into account the business strategy, the size of the organization, the structure of the organization and more. The plan must include, among other things, reference to the following issues: the declaration of a cyber incident and the definition of the incident level, the structure and staffing of situation rooms, communication channels, bodies and designated work processes.

The actions required in the stages of event management (from identification to recovery):

- Technological
- Business and Legal.
- Assistance from government agencies and work with regulators and law enforcement authorities.
- Table of readiness and qualifications.
- Announcement of termination of a cyber incident.

Skilled attackers will perform deceptive actions, so it can sometimes long time before the real problem is identified. The first stages of handling the incident is to characterize the attack under lack of information - what exactly happened, what is the real damage, who the attacker is/was and what he wanted.

In an environment of technological uncertainty, the organization is exposed to business, legal risks and of course the risk of reputational damage. Therefore, the organization's response is critical and requires a variety of decisions that should be made at this stage correctly and quickly, such as: what messages are conveyed to customers, employees, authorities, and the media.

The aim of the course is to learn and experience complex cybersecurity events, understanding the tools and technologies for dealing with business questions and challenges in the digital age. The course deals with the study and analysis of cyber events and data while focusing on the organization and the business continuation during the cyber-attacks. We will review business problems and challenges from different fields and we discuss ways to make the right managerial decisions during the cyber-attacks. We will learn different methodologies, methods and technologies.

The course is based on several components:

- Lectures and class discussions - The course presentations will be published on the course website (http://moodle.tau.ac.il). Please notice that the slides presented on the website do not include all the material that will be presented and discussed in class.
- Supplementary reading and analysis of articles - During the semester, relevant articles will be published on the website, which will form the basis for class discussion. The articles should be read before the lesson date.
- Guest lectures - The course will be accompanied by leading lecturers from industry and academia who will cover various topics in the field of cybersecurity.
- Student presentations (depending on progress)
- Explanations regarding the concluding project.

**Project concludes**

During the course period the students will work on the concluding project. The project will address a cybersecurity business problem as close to reality as possible (for example: dealing with a cyber-attack on the organization or/and preparing the organization for a cyber-attack).

## Assessment and Grade Distribution

| Percentage | Assignments | Due Date | Group's size |
|---|---|---|---|
| 10% | Active participation | Throughout the course | Individual |
| 20% | Written Assignment | Will be provided at the beginning of the course | Groups of 2 students |
| 70% | Final Project | 2 weeks after the semester ends | Groups of 2 students |

This class relies on active yet judicious student participation. Students will have the opportunity to discuss the role of ethics in business in a safe environment with their peers. My goal is that everyone will contribute to the discussion (and get a good participation grade). Above-average participation grades will denote consistent, timely and astute observations, answers, or comments, which clearly elevate everyone’s learning experience. Below-average participation grades will denote either lack of participation or excessive/disruptive comments that prevent others from getting the most of the class. Note that your participation grade will also be affected if you miss any class session(s), unless justified (such as in case of reserve duty).

- According to University regulations, a student must be present in every lesson (Article 5).

- The lecturer reserves the right to have a student removed from a course if the student is absent from a class with mandatory participation or did not actively participate in class. (The student will remain financially responsible for the course irrespective of his/her removal from the course).

## Course Assignments

- Students are required to submit written assignments and the final project.
- Should a student become unable to complete an assignment or course requirement, s/he must notify the TA/Lecturer of the course in advance via email.

## Grading Policy

As of the 2008/9 academic year the Faculty has implemented a grading policy for all graduate level courses. This policy applies to all graduate courses in the Faculty, and will be reflected in the final course grade. Accordingly, the final average of the class for this course (which is a core course) will fall between 83-87%. Additional information regarding this policy can be found on the Faculty website.

## Evaluation of the Course by Student

Following completion of the course, students will participate in a teaching survey in order to evaluate the instructor and the course for the benefit of the students and the university.

## Course Site (Moodle)

- The course site will be the primary tool used to communicate messages and material to students. It is, therefore recommended to periodically check the course site in general, periodically, before each lesson, at end of thecourse, as well. (For example: final project details and updates regarding assignments).
- Course slides will be available on the course site.
- Please note that topics which are not covered in the slides, but are discussed in class are considered an integral part of the course material and may be tested in the class assignments.

## Course Outline*

| Session | Topic(s) | Comments |
|---|---|---|
| 1 | Course overview and introduction, what has changed in the world of information security and in the cyber economy space, increasing organizational awareness | Preparation guidelines<br>The reading materials will help you to expand your knowledge of the materials presented in this module |
| 2 | Protection strategy in the framework of cyber risk management, preliminary assessments, cases and reactions during a cyber incident, actions after the incident | Preparation guidelines<br>The reading materials will help you to expand your knowledge of the materials presented in this module |
| 3 | Cyber protection management, risk management, business continuity management, information technology management, training and practice | Preparation guidelines<br>The reading materials will help you to expand your knowledge of the materials presented in this module |
| 4 | Guest lecture, continuing tutorials and practice | Preparation guidelines<br>The reading materials will help you to expand your knowledge of the materials presented in this module |
| 5 | Management of cyber protection in the supply chain, control objectives and cyber protection controls | Preparation guidelines<br>The reading materials will help you to expand your knowledge of the materials presented in this module |
| 6 | Cyber drill simulation | Preparation guidelines<br>The reading materials will help you to expand your knowledge of the materials presented in this module |
| 7 | Student presentations | Preparation guidelines<br>The reading materials will help you to expand your knowledge of the materials presented in this module |

*Subject to changes

## Required Reading


1. The Complete Guide to Cybersecurity Risks and Controls by Anne Kohnke, Dan Shoemaker, Ken Sigler, 2017
2. EU Cybersecurity Act, European Parliament, 2019
3. Insider Threat Report, Verizon, 2019
4. Cybersecurity Impact on Insurance Business and Operations, Thomas Hartl, Kevin Olberding, David Schraub, 2017
5. IOCTA 2016, INTERNET ORGANISED CRIME THREAT ASSESSMENT, Europol
6. Mitigating Security Risks Through Attack Strategies Exploration; Braham Lotfi Mediouni, Ayoub Nouri, Marius Bozga, Axel Legay, and Saddek Bensalem, 2018
7. Guidelines on assessing DSP (digital service providers) and OES (operators of essential services) compliance to the NISD security requirements, ENISA, 2018
8. Measuring the Cost of Cybercrime, Ross Anderson, Richard Clayton, Chris Barton, Rainer B¨ohme, Michel J.G. van Eeten, Stefan Savage, Michael Levi, Tyler Moore, 2012
9. Cost of community violence to hospitals and health systems; Jill Van Den Bos, Nick Creten, Stoddard Davenport, Mason Roberts, 2017
10. The Behavioral Economics Guide, Alain Samson, Dan Ariely, 2015


## Recommended Reading


11. Gray Hat Hacking, the Ethical Hacker's Handbook, Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, and Terron Williams, 2011
12. Cybersecurity, Managing Systems, Conducting Testing, and Investigating Intrusions, Thomas J. Mowbray, PhD, 2014
13. Penetration testing, Georgia Weidman. 2014