CEU Department of Economics and Business

CENTRAL EUROPEAN UNIVERSITY

Syllabus

Security and Data Protection course

- **Instructor:** Peter Papp (tel: +36205504108, email: peter@papp.com, office hours: 24/7)
- **Credits:** 1 (2 ECTS)
- **Term:** Winter 2017-2018
- **Course level:** MSc
- **Prerequisites:** Basic knowledge of IT management and corporate business processes

Course availability

Cap: 25. Students from the MS in Business Analztics and MS in Technology Management and Innovation programs will have direct entry (priority 1) upon registration.

Course description

The main objectives of Security and Data Protection course may be summarised as:

- Giving an overview about the role of CISO (Chief Information Security Manager)
- Helping to designing an IT security policy (how to collaborate with customer and suppliers, how to align with the needs of the business.)
- Helping to ensure compliance with the IT security standards.
- Explaining the role of the risk management systems.
- Teaching how to be proactive and evaluate in advance the security risks that may arise from changes made to the infrastructure, new lines of business, etc.

Learning outcomes

Core Learning Area	Learning Outcome
Interpersonal Communication Skills.	Students will be able to communicate about the role and responsibility of IT security issues also with IT managers and also with business managers.
Technology Skills	Students will get an overview about today's IT security standards and also about best-of -breed IT security tools.
Cultural Sensitivity and Diversity	Students will have increased understanding about the relevance of diversities of IT security policies in different countries.
Quantitative Reasoning	Students will learn how to deal with business and IT security trade off.
Critical Thinking	Students will be encouraged to question the necessity of an IT/IT security investment and

	also to encourage the implementation of the must have IT security.
Ethics and Responsibility	Students will be motivated to consider the business limitations of IT security.
Management Knowledge and Skills	Non-specialist managers will have a clear understanding of the necessity and role of the IT security in enterprises.

Reading list

James Borg: Persuasion, the art of influencing people

Shon Harris, Allen Harper, Chris Eagle, Jonathan Ness, Michael Lester: Gray Hat Hacking - The Ethical Hacker’s Handbook

John Viega: The Myths of Security (what the computer security industry doesn’t want you to know)

Bruce Schneier: About Security

http://en.wikipedia.org/wiki/Sarbanes-Oxley_Act

Mikko Hypponen TED talk: How the NSA betrayed the world’s trust – time to act

http://www.ted.com/talks/mikko_hypponen_how_the_nsa_betrayed_the_world_s_trust_time_to_act

Joe McCray Hacktivity talk - Big Bang Theory - Pentesting high security environments

https://www.youtube.com/watch?v=qBVThFwdYTc

Bruce Schneier, Hacktivity 2010 keynote speak.

https://vimeo.com/27190504

Jeff Bardin, Hacktivity 2012: So You Want To Be A Cyber Spook

https://www.youtube.com/watch?v=c7cULobYCsQ

Ákos Subecz , Hacktivity 2012 - Security Problems at Hungarian everydays (lockpicking)

https://www.youtube.com/watch?v=5ssR5WtpnN0

Assessment

The course grade will be based on a number of different evaluation elements.

- Class attendance and participation: 40%
- Minute paper (one time, at last session, 30 minutes, 5 questions): 30%
- Homework (preparing and presenting one TED like presentations about a relevant IT security topic) 30%

Grades		%
A	Outstanding	96-100
A–	Excellent	90-95
B+	Very good	85-89
B	Good	80-84
B–	Satisfactory	75-79
C+	Minimum Pass	60-74
F	Fail	0-59

The above table serves as a generic example of the scaling applied: in line with the CEU grading policies the instructor reserves the right to adjust the scale, that is, to grade on a "curve", should he find that significantly more than the usual number of students would not pass the course under the indicated grading scale or should the distribution of the grades represent an unrealistic pattern.

Class participation – 40%

40% of the grading points will be earned by a student for class participation.

Class activities include:

- Evidence of preparation,
- Contributions to class discussion,
- Bringing real life examples, based on own working experience,
- Short voluntary presentation/briefing on cases from own research (newspapers, web, etc.) in context with the topic of the particular or previous class These points are necessarily subjective by nature. The instructor will do his best to be as fair as possible but this grading element is not open for discussions. If class attendance is below 60% for an individual, 0% is assigned to class participation.

Minute paper: - 30%

Homework: TED like presentations about a relevant IT security topic: 30%

We’ll choose hot IT security topics from the last two month and students in groups (2-3 people) have to prepare and present a 5-6 minutes presentation/speech about it. This “game” simulates how a CISO should present an IT security issue to board members and how to convince the board members about the business importance of an IT security issue.

Course schedule and materials for each session

1.	6th of February 5.30 pm – 8.00 pm	**How Security (Should) Work in Real Life** • Introductions of the instructors • How the course will be conducted • The man and the security • How the media changed security in today life • How to deal with security today
2.	20th of February 5.30 pm – 8.00 pm	**IT Security Standards and GDPR** • Definitions: standards, recommendations, models • IT security and law • ISMS (Information Security Management System) • ISO 27000 series
3.	26th of February 5.30 pm – 8.00 pm	**Ethical Hacking** • What is ethical hacking • How it works in real life • Legal issues • Ethical hacking tools Invited speaker
4.	27th of February 5.30 pm – 8.00 pm	**Social Engineering** • What is social engineering? • History of social engineering • Types of social engineering • Show me a social engineer Invited speaker