Syllabus template

Notes to instructors:

All text in italics are suggestions to you, that you should delete or replace in preparing your own course-specific information, before distributing the syllabus to students or making it available on the intranet. (Please delete this page entirely.)

Syllabi for courses already offered at the Business School (not necessarily complying with this template) are available for reference on the Q drive, under Syllabi and the Semester in which they were last taught.

CEU Business School

BUSI 5607- Security and Data Protection
(*1,5 credits*)
MSc in Business Analytics

Instructor	Peter Papp
Class meets (day and time):	see timetable for exact dates
Classroom:	according to the schedule
Office:	
Tel:	+36205504108
Fax:	+3602704fax
E-mail:	peter@papp.com
Office hours:	24/7
Program Coordinator:	Zoi Hrisztodulakisz (hrisztodulakiszz@business.ceu.edu)

---

1. PREREQUISITIES

Basic knowledge of IT management and corporate business processes.

2. POLICY ON ADMITTING NON-MBA STUDENTS

It is the general policy of the Business School to admit students from other units of CEU, provided that the prospective student meets the course perquisites stated above

3. COURSE OBJECTIVES

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.

5. MAIN TOPICS

- How Security (Should) Work in Real Life
- IT Security Standards
- Ethical Hacking
- Business Continuity and Contingency Plan
- IT Security Tools
- Social Engineering

6. INTENDED 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.

7. HOW THE CLASS SESSIONS WILL BE CONDUCTED

Each class will be a combination of lectures and interactive sessions, incl. guest speaker presentations, student team debates and student project presentations. Often students will be asked to briefly summarize in class one of the topics presented. A number of real world examples, cases, and articles will be used to demonstrate the topics discussed. Invited guest speakers (IT managers, IT security consultants) will strengthen the real business life focus of the course. Students are encouraged to read

IT security journals and web sources and volunteer to present short cases of interest in conjunction with the topics of the course.

8. POLICY ON THE AVAILABILITY OF LECTURE NOTES

Keynote presentations will be available on the day of classes.

9. GRADING

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

- Class attendance and participation 40%
- Minute papers or homework 30%
- TED like presentations about hot IT security topics 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 papers or homework - 30%

TED like presentations about hot IT security topics 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.

10. ACADEMIC INTEGRITY

The Business School expects all students to adhere to the fundamental principles of academic integrity in any and all behaviours associated with their course work and otherwise, as stated in the CEU Honor Code (see Student Handbook). Attempted cheating of all forms is treated extremely seriously and can result in dismissal from the School and University.

11. RECOMMENDED READINGS AND OTHER SOURCE MATERIALS

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

15. COURSE OUTLINE AND SESSION ASSIGNMENTS

1.	October 8 12:30-15:30	**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.	October 9 12:30-15:30	**IT Security Standards** • Definitions: standards, recommendations, models • IT security and law • ISMS (Information Security Management System) • ISO 27000 series
3.	October 9 16:00-19:00	**Ethical Hacking** • What is ethical hacking • How it works in real life • Legal issues • Ethical hacking tools Invited speaker
4.	November 6 9:00-12:00	**Business Continuity and Contingency Plan** • Definitions • BCCP and Disaster Recovery Plan • BCCP legal issues • Sample BCCP • How to maintain a BCCP Invited speaker
5.	November 6 12:45-15:45	**IT Security Tools** • Type of tools • Licences • How and when to use? • How reverse engineering is working? Invited speaker
6.	November 6 16:00-19:00	**Social Engineering** • What is social engineering? • History of social engineering • Types of social engineering • Show me a social engineer Invited speaker

16. BRIEF BIO OF THE INSTRUCTOR

Peter Papp is a well-known business professional working in IT security area and acting also as business angel. He graduated at ELTE (Budapest, Hungary) as programmer mathematician. He studied at The Open University Open Business School (Professional Certificate in Management; and Professional Diploma in Management). For the time being he is Honorary Associate Professor at National University of Public Services and

actively working in different IT security areas. He is the CEO of kancellar.hu, leading IT security firm in Hungary, and co-owner in Hacktivity, the biggest IT security Festival in CEE.
He was a TEDx speaker and for the time being as a "hobby" he is the CEO and co-owner for TEDxDanubia in Hungary.