CYBERSECURITY & IT RISK MANAGEMENT

BACHELOR IN MANAGEMENT INFORMATION SYSTEMS

Professor: ANDER ORTIZ ORTEGA
E-mail: aortizo@faculty.ie.edu

Academic year: 18-19
Degree course: THIRD
Semester: 2º
Category: COMPULSORY
Number of credits: 6.0
Language: English

PREREQUISITES
The student should have knowledge of the following areas (which correspond to subjects of the BIS program):

- Databases and data modelling
- Operating Systems
- Programming, data structures and algorithms
- Software development
- Information systems analysis and design
- Enterprise management information systems
- HW, SW & systems infrastructure
- Project Management

SUBJECT DESCRIPTION
Globalized, regulated, competitive and socially responsible companies demand strong internal control structures and processes that set the goals, measure the performance and handle deviations against technologically supported services that impact end users. In this context, the IT risk management discipline focuses on understanding, assessing, preventing and managing the main threats that can harm the reliability and security of the IT systems that support business processes in any kind of organization.

The current ‘hyper-connected’ landscape of digitalized business and tech-friendly users inevitably opens the critical IT infrastructure of companies to Internet in order to meet new requirements of efficient and flexible business models such as B2C, B2B, outsourcing, cloud computing, managed services (like SaaS, PaaS or IaaS), teleworking or on-demand virtualization servers and workstations, among others. Thus, this challenging environment exposes companies to mature, evolving and complex cyber threats developed by organized threat actors such as states (cyber warfare), cyber activism and competitors, as well as for advanced users that master the fundamentals of ethical hacking. For this reason, cybersecurity becomes one of the most important strategic risks for the reputation, stability and business continuity of relevant organizations.

OBJECTIVES AND SKILLS
This course aims to set the fundamentals about the risk management principles for technology-supported businesses, the use of control-based approach to prevent and/or minimize the harm of prioritized risks, and the breakdown of cybersecurity techniques and skills as a mean to proactively respond to cyber risks while minimizing the impact on business operations, stability and reputation. IT risk management and cybersecurity-related roles inside an organization.

At the end of the course, you should be able to:

- Provide the foundation for identifying, analyzing and managing IT risks throughout usual business operations, using different methodologies and techniques commonly applied by corporations and according to standards of good practice.
- Understand the different roles involved in IT risk management inside an organization and their corresponding responsibilities and liaison with business representatives.
- Learn and apply the best market practices for enabling processes and organizational structures that are resilient to IT risks according to IT governance and risk management principles, in line with business objectives and priorities.
- Provide the technical skills and management abilities for defining overarching cybersecurity programs that protect IT assets and digitalized business information from advanced cyber security threats, based on the application of IT-risk-oriented cybersecurity controls, processes and resources.
- Practice with hands-on cybersecurity labs in order to think as an ethical cyber-attacker (white-hat hacker) but act as a cyber-defender (blue teams) according to ethical and audit behavior and restrictions.
- Rehearse the security-related roles (such as CISO, CIO, IT Audit and IT Risk) and groups of interest (such as SOCs or CSIRTs) in evolving and collaborative case-oriented exercises by groups that develop different areas of expertise and foster their relationship with business areas.
- Present your own business case about a real-life cyber incident occurred and how can this be solved through a bespoke IT risk management and cybersecurity program.

METHODOLOGY

All the sessions will be included in a continuous evaluation process, with some milestones with exercises and practices. Hence, a combination of lectures and practical classes will be used.

<table>
<thead>
<tr>
<th>Teaching methodology</th>
<th>Weighting</th>
<th>Estimated time a student should dedicate to prepare for and participate in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lectures</td>
<td>20.0 %</td>
<td>30 hours</td>
</tr>
<tr>
<td>Discussions</td>
<td>13.33 %</td>
<td>20 hours</td>
</tr>
<tr>
<td>Exercises</td>
<td>20.0 %</td>
<td>30 hours</td>
</tr>
<tr>
<td>Group work</td>
<td>20.0 %</td>
<td>30 hours</td>
</tr>
<tr>
<td>Other individual studying</td>
<td>26.67 %</td>
<td>40 hours</td>
</tr>
<tr>
<td>TOTAL</td>
<td>100.0 %</td>
<td>150 hours</td>
</tr>
</tbody>
</table>

20th December 2018
PROGRAM

SESSIONS 1 - 2
Introduction to the course.
Introduction to cyber security.
BUSINESS CASE (work in groups): Cybersecurity roles and responsibilities.

SESSIONS 3 - 4
Introduction to IT risk management
BUSINESS CASE (work in groups): IT roles and their responsibility on cybersecurity. The pain points of the study case company: processes, critical assets, value (impact) on business.

SESSIONS 5 - 6
IT risk management foundation: IT governance.
BUSINESS CASE (work in groups): Threats for the study case company, likelihood, applicability to asset types and vulnerabilities. Environmental conditions to consider regarding the impact.

SESSIONS 7 - 8
Implementation and monitoring of IT risk management function.
Secure Systems Development Life cycle
ROLE PLAY: SSDLC and IT/Cybersecurity roles.
- Practical exercise combining IT Risk management principles and IT functions’ roles & responsibilities. To be developed in groups according to the different roles that will be rehearsed, and presented altogether during the class. A written plan (objectives, requirements, strategy to follow) for each role (group) will be collected and evaluated before it is played.

SESSIONS 9 - 10
Cyber security governance and strategy.
Cybersecurity rules and documental frameworks.

SESSIONS 11 - 12
Cyber security management systems.
Social engineering.
Training and awareness.
BUSINESS CASE (work in groups): Development of a training & awareness program for the study case company. Metrics and KPIs of activities within the training & awareness program.

SESSIONS 13 - 14

---

20th December 2018
Identification, authentication and authorization.
Role-based access control.
Identity & Access Management.
BUSINESS CASE (work in groups by students): The CEO fraud. Description of real incidents, identification of security flaws for each business process affected and define a remediation plan in the medium/long term. A documented presentation will be required by each group.

SECTIONS 15 - 16
Mid-term exam.
BUSINESS CASE (work in groups by students): The CEO fraud. Presentation of results.

SECTIONS 17 - 18
Cybersecurity compliance.
BUSINESS CASE (work individually after the class): Identification of payment data in affected processes of the study case company. Definition of IT Security controls. Identification of evidences of compliance. The work will be collected in the following week.

SECTIONS 19 - 20
Ethical hacking.
HANDS-ON CYBERSECURITY LAB (work individually in class): Network attacks and countermeasures.

SECTIONS 21 - 22
Web hacking.
HANDS-ON CYBERSECURITY LAB (work individually in class): Web attacks and countermeasures.

SECTIONS 23 - 24
Cybersecurity monitoring and operations.
Network security baseline assurance.
BUSINESS CASE (work in groups): Definition of SOC services catalog for the study case company.

SECTIONS 25 - 26
Endpoint security baseline assurance
Criptography.
Data privacy and protection.
HANDS-ON CYBERSECURITY LAB (work individually in class): Data-loss prevention scenario.
SESSIONS 27 - 28
- Business continuity plans.
- IT continuity of business operations.

BUSINESS CASE (briefing by professor): EQUIFAX CASE. Identification of action plans as a result of the briefing. The results will be collected and evaluated.

SESSIONS 29 - 30
End-term exam.
Cyber resilience:
- Incident response life cycle.
- Digital Forensics.
- Cyber wargames.

Closing remarks of the course.
PRACTICAL EXERCISE (to be worked in groups): Design of a cyber wargame.
**BIBLIOGRAPHY**

Lecture slides, exercises, documentation and any additional reads needed to follow this subject will be posted as the course progresses.

**RECOMMENDED**

For students looking for basic learning and reinforce essential security skills quickly I recommend this straight-forward guide designed in 3 volumes to speed learning and information retention.

[http://www.hackerhighschool.org/books.html](http://www.hackerhighschool.org/books.html)

1. Nige the Security Guy
[https://nigesecurityguy.wordpress.com/](https://nigesecurityguy.wordpress.com/)


3. CISO soft skills: securing organizations impaired by employee politics, apathy, and intolerant perspectives
[https://ie.on.worldcat.org/oclc/435607323](https://ie.on.worldcat.org/oclc/435607323)

**EVALUATION CRITERIA**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Percentage</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class Participation</td>
<td>25 %</td>
<td>Students are expected to identify from public sources and prepare the upcoming topics that will be presented the week before. Discussions and quizzes will be maintained at be beginning of the class to check this requirement.</td>
</tr>
<tr>
<td>Group Presentation</td>
<td>25 %</td>
<td>Students are expected to attend and understand instructions for each exercise, work in groups, select the appropriate spokesperson, agree and document the outcomes, and (in case of spokesperson) present it in class on behalf of the rest of the group. Quality, completeness and alignment with class topics will be the criteria to evaluate this requirement.</td>
</tr>
<tr>
<td>Intermediate Tests</td>
<td>20 %</td>
<td>Mid-term exam.</td>
</tr>
<tr>
<td>Final Exam</td>
<td>30 %</td>
<td></td>
</tr>
</tbody>
</table>

**PROFESSOR BIO**

Professor: **ANDER ORTIZ ORTEGA**

E-mail: aortizo@faculty.ie.edu

20th December 2018
ANDER ORTIZ ORTEGA

Ander Ortiz is a professional with more than 14 years of experience in risk management, business resilience, information security, internal control, information systems management and external audit.

Ander is senior manager in Deloitte, which he joined in 2006. He is currently the head of Cyber Resilience services for Spain, focused on preparation, response and testing against complex cyber threats. In the past, he assumed the role of leading Information Privacy & Protection, and Identity & Access Management service lines in Spain.

He holds a master’s degree in Information Security from University of Deusto and a Computer Science Engineering degree at the same University. Other certifications and courses are:

- CISA (Certified Information Systems Auditor), ISACA.
- CISM (Certified Information Security Management), ISACA.
- CISSP (Certified Information Systems Security Professional), ISC(2).
- ISO 27001 Lead Auditor, exam passed.
- BS25999 Lead Auditor (current ISO 22301), exam passed.
- EC-Council CEH (Certified in Ethical Hacking), exam passed.

So far he has combined his work in Deloitte with part-time associate professor for Cybersecurity, Business & IT Resilience, IT Governance and IT Audit for several institutions for the last 14 years (University Carlos III of Madrid, University of Deusto).

OTHER INFORMATION

The best way to arrange a meeting with me, is by sending me an email to this address: aortizo@faculty.ie.edu.

CODE OF CONDUCT IN CLASS

1. **Be on time**: Students arriving more than 5 minutes late will be marked as “Absent”.

   Only students that notify in advance in writing that they will be late for a specific session may be granted an exception (at the discretion of the professor).

2. **If applicable, bring your name card and strictly follow the seating chart**. It helps faculty members and fellow students learn your names.

3. **Do not leave the room during the lecture**: Students are not allowed to leave the room during lectures. If a student leaves the room during lectures, he/she will not be allowed to re-enter and, therefore, will be marked as “Absent”.

   Only students that notify that they have a special reason to leave the session early will be granted an exception (at the discretion of the professor).

4. **Do not engage in side conversation**. As a sign of respect toward the person presenting the lecture (the teacher as well as fellow students), side conversations are not allowed. If you have a question, raise your hand and ask it. It you do not want to ask it during the lecture, feel free to approach your teacher after class.

   If a student is disrupting the flow of the lecture, he/she will be asked to leave the classroom and, consequently, will be marked as “Absent”.

5. **Use your laptop for course-related purposes only**. The use of laptops during lectures must be authorized by the professor. The use of Social Media or accessing any type of content not related to the lecture is penalized. The student will be asked to leave the room and, consequently, will be marked as “Absent”.

20th December 2018
6. **No cellular phones**: IE University implements a “Phone-free Classroom” policy and, therefore, the use of phones, tablets, etc. is forbidden inside the classroom. Failing to abide by this rule entails expulsion from the room and will be counted as one absence.

7. **Escalation policy: 1/3/5.** Items 4, 5, and 6 above entail expulsion from the classroom and the consequent marking of the student as “Absent.” IE University implements an “escalation policy”: The first time a student is asked to leave the room for disciplinary reasons (as per items 4, 5, and 6 above), the student will incur one absence, the second time it will count as three absences, and from the third time onward, any expulsion from the classroom due to disciplinary issues will entail 5 absences.