



---

## 2IN1520 – Risk analysis - INFOSEC

---

**Instructors:** Valerie Viet Triem Tong

**Department:** CAMPUS DE RENNES

**Language of instruction:** FRANCAIS

**Campus:** CAMPUS DE RENNES

**Workload (HEE):** 40

**On-site hours (HPE):** 27,00

---

### Description

This week of courses alternates between lectures and practical case studies to present cyber risk analysis. A cyber security risk analysis is about understanding, managing, controlling and mitigating cyber risk across a digital organization. Risk analysis a crucial part of data protection efforts.

### Quarter number

semaine bloquée en fin de SG8

### Prerequisites (in terms of CS courses)

none

### Syllabus

#### Threat Analysis

who the attackers are, what are their motivation and organisation,  
their characteristics  
Cyber Threat Intelligence  
Study of some APTs

#### Risk analysis

- purpose of risk analysis
- presentation of different approaches
- focus on Ebios-RM

#### Technical security

#### Legal framework

#### Physical Security

Study of the modus operandi of attacks exploiting vulnerabilities in the implementation of physical security



## **Security in the Industrial sector**

### **Crisis management**

Practical study of three cases of cyber-attacks and the coordination of the response of internal and external actors in the management of the related crisis.

- Crisis management process (Attack against TV5 Monde)
- Crisis communication (Attack on Norsk Hydro)
- Remediation (NotPetya attack against Maersk)
- 

### **Social Engineering**

Analysis of pressure tactics based on social engineering techniques

### **Class components (lecture, labs, etc.)**

A week with some traditional classes and lots of interaction with lecturers through

Concrete situation on many small examples

Practical case studies in small groups and feedback to the whole group

Discussion with Philippe Thomazo, CEO of the ECOCERT group who will testify on his experience of cyber risks.

### **Grading**

Evaluation of written knowledge with the help of a quiz and via oral restitution of the case studies made during the week.

### **Resources**

Course materials, videos, testimonials, case studies

### **Learning outcomes covered on the course**

Taking into account the Cyber risk

Assessing the real impact of a cyber-attack on the company's business

Understanding the threat organization

Consider the different aspects of cyber crisis management

### **Description of the skills acquired at the end of the course**

At the end of this course, the student will master the stakes, the steps and the means of a risk analysis in a digital organization. He/she will be able to reconstitute it to different instances of the organization (technical, organizational and decisional).