



GNAM Elective: Digital Resilience

1. COURSE OBJECTIVES AND METHOD

We are in a period of unprecedented technological change - disruptive technologies such as Internet of Things (IoT), mobile, and big data are already changing how businesses operate, strategize and communicate. As more organizations digitize their processes with these technologies, they are realizing that operating reliable digital services and safeguarding sensitive data are essential to establishing trust with customers and maintaining business continuity.

Any organisation that relies on computer networks, digital information, and the Internet is vulnerable to cyber-attacks. Sabotage, hacking, even uncontrolled use of social media: all these can lead to financial loss, disruption of operations, and, inevitably, reputational damage. The threats are real, and they are changing all the time. Managing these threats is not the sole responsibility of the IT department, it is business leaders' job to understand and oversee organisations' response to cyber/digital threats and attacks.

With an ever-increasing number of security breaches and privacy incidents under the spotlight, consumers' awareness about privacy is also becoming significantly higher. Consumers are starting to act based on how well they believe their privacy is protected by the organizations collecting and processing their personal information. Thus, customer trust is becoming the most important asset of companies doing digital business. The challenge is not only the security incidents or customer expectations, but also the changing regulations. As an example, the new General Data Protection Regulation (GDPR) is effective since May 2018, imposing stricter rules to companies handling personal data. Organizations that fail to provide secure means of data collection and analysis will be facing high fines. Compliance with any data protection regulation affects every department and require input from CMOs, CEOs, and boards, in addition to cyber security teams.

Considering the above-mentioned trends, the objective of this course is to introduce the participants to the fifth dimension of warfare: the cyber arena. This course will help participants build awareness about cyber threats they are likely to experience, the data security & protection compliance challenges they will face, the operational as well as ethical dilemmas they will need to address, and, crucially, what actions to take in case of cyber incident.

Participants will learn about digital technologies and how to create a digital strategy, as well as how to bring these technologies into the organization to create value. This elective covers this gap by bringing cross-disciplinary expertise together on domains such as cyber security, privacy, digital consumer behaviour, and, compliance and ethics, so that participants are informed about trust building practices in the digital domain. At the end of this course, participants will become intelligent consumers of the advice provided by Chief Security Officers (CSOs) or external consultants. Participants do not need any previous knowledge in IT or cyber security: the focus is on general managers and directors.

The learning objectives of the course are as follows:

- Understand the cyber security threats that organizations are exposed to, and be able to communicate them effectively to the rest of the leadership team or the board,
- Recognize the importance of treating cyber security at the board level,
- Recognize the new consumer trends in privacy and data protection,
- Understand what the data protection regulations mean for businesses,
- Be prepared for the dilemmas in case of an incident, and have strategies for responding.

2. COURSE MATERIALS

This course does not have an assigned textbook. The required readings will be in the form of articles and research reports, both from academic and non-academic resources. These mandatory readings will be delivered to you before the sessions.

Some of the sessions come along with a case or article that you need to read prior to class. To maximize your learning in class I recommend that you give some thought to the discussion questions provided along with the case (if any). All cases will be discussed in class. Additional reading material may be available for each session. None of these readings is mandatory, yet, they are interesting as background material.

3. COURSE OVERVIEW

DATE/TIME	DURATION	TOPIC	MATERIAL
06.09.2024 2 - 5.30 PM CET	2 x 90 min w/ 30 min break	Introduction to the course Cyber Threat Landscape Cybersecurity strategy	Read; https://cmr.berkeley.edu/2024/07/getting-cybersecurity-right/
13.09.2024 2 - 5.30 PM CET	2 x 90 min w/ 30 min break	Cyber incident management and handling	Read; iPremier Case A Supplemental; https://sloanreview.mit.edu/article/the-ransomware-dilemma/
27.09.2024 2 - 5.30 PM CET	2 x 90 min w/ 30 min break	Privacy & Changing consumer expectations Guest Speaker on “Social engineering and Incident Handling Best Practices”	
04.10.2024 2 - 5.30 PM CET	2 x 90 min w/ 30 min break	Privacy by Design Guest Speaker on "Governing privacy" – <i>TBC</i>	Read; "Customer Data: Designing for Transparency" by Morey et al., HBR 2015
25.10.2024 2 - 5.30 PM CET	2 x 90 min w/ 30 min break	Digital Ethics Guest Speaker on “Operationalizing Digital Ethics” <i>TBC</i>	Read; https://hbr.org/2024/05/4-types-of-gen-ai-risk-and-how-to-mitigate-them
01.11.2024 2 - 5.30 PM CET	2 x 90 min w/ 30 min break	Corporate Digital Responsibility Course wrap-up	Read; Corporate Responsibility in the Digital Era, MIT SMR, M. Wade, April 2020

4. ASSESSMENT

You will be assessed based on the following items;

Assessment	Impact on grade
Participation	20%
Multiple choice quiz on cybersecurity (at the end of 2 nd session)	10%
Discussion post on data protection regulations (due by session 3)	10%
Group assignment – Privacy by Design Case Analysis (to be started during Session #3)	20%
Individual written assignment in the form of case analysis, where students will need to apply the knowledge from this course to analyze and answer questions that will come with the case. More information on the case and submission expectations will be announced later on.	40%

Attendance & Participation:

- In addition to the above elements, attendance will impact your grade. Missing two sessions of six, unexcused, will lead to a failing grade.
- Joining sessions late or leaving sessions early will only be allowed for valid excuses that were communicated and explained in advance. Otherwise, only one instance of tardiness will be tolerated, and the second one onward will lead to grade penalty.
- Given the virtual nature of the course, having your camera on is an expectation, and it is considered to be part of the attendance.
- Participation and attendance are not the same. I expect your full attendance and participation.
- This course does not work well with multi-tasking given the high quantity of plenary and in-group discussions. Please be prepared to contribute to discussions, learn from your peers, and note that you may be cold called to share your point of view.

5. CONTACTS

The fastest way to reach me is via e-mail. For any questions or concerns you have, or to make an appointment please send an e-mail to oyku.isik@imd.org.
