הפקולטה לניהול ע"ש קולר אוניברסיטת תל אביב

Coller School of Management Tel Aviv University

The Leon Recanati Graduate School of Business Administration

1242.3257.01 – Information and Cyber Security

Second Semester – 2020/21

Tentative syllabus

Section	Day	Hour	Final Task	Lecturer	Email	Telephone
01	Tuesday	18:45-21:30 **(Second half)**	Exam	Dr. Nimrod Kozlovski	nimrod.kozlovski@gmail.com	

This course is given in **HEBREW**

Course Units

1 course unit = 4 ECTS units

The ECTS (European Credit Transfer and Accumulation System) is a framework defined by the European Commission to allow for unified recognition of student academic achievements from different countries.

Course Description

1. This course aims to provide executive leadership with a high-level overview of various aspects of Cybersecurity in the context of current threats and characteristics of the cyber domain.
2. Through lecture, demonstrations, and group discussion, the attendance will gain a foundational perspective on the challenges of designing a cybersecurity program, implementing secure systems, and other factors needed for a comprehensive cybersecurity solution.
3. The course will allow to the attendance to integrate core fundamentals of cyber security into business cases, and test cyber incidents from a different aspect. Today's business environment force executive to address data security and cyber issues on a daily bases, while gaining basic understanding one can improve his management skills though independent thinking process without relying on his CTO.
4. Each of the training days will contain two of the following elements:
    a. Intro to the subject – the first part of the day allows the attendance to be familiar with key elements of each topic, understand the general framework and get.

b. Business case and simulation analysis – While analyzing and working on real life events, the attendee will apply the knowledge they gained in the first part of the day. The analysis will focus on the elements, such as, but not limited to; understanding the attacker kill chain, management of the in house response team, handle with relevant outsource parties, applying the organizational business recovery plan, using the right technological tools and more.
c. Lesson learnt

Course Objectives

Upon completion of the course, the student will be able to:

1. Understand cyber risks from management perspective
2. Analyze cyber readiness and cyber incident response action
3. Understand cyber operation from corporate perspective
4. Realize the evolving cyber regulation

Evaluation of Student and Composition of Grade

Percentage	Assignment	Date	Group Size/Comments
100%	Final Exam		

* Students who absent themselves from classes or do not actively participate in class may be removed from the course at the discretion of the lecturer. (Students remain financially liable for the course even if they are removed.)

Grading Policy

In the 2008/9 academic year the Faculty instituted a grading policy for all graduate level courses that aims to maintain a certain level of the final course grade. Accordingly, this policy will be applied to this course's final grades.
Additional information regarding this policy can be found on the Faculty website.
https://coller.tau.ac.il/MBA-students/programs/2020-21/MBA/regulations/exams

Evaluation of the Course by Student

Following completion of the course students will participate in a teaching survey to evaluate the instructor and the course, to provide feedback for the benefit of the students, the teachers and the university.

Course Site (Moodle)

The course site will be the primary tool to communicate messages and material to students. You should check the course site regularly for information on classes, assignments and exams, at the end of the course as well.

- Course material will be available on the course site.
- Please note that topics that are not covered in the course material but are discussed in class are considered integral to the course and may be tested in examinations.

Course Outline*

Module 1 - Cyber security paradigms – understanding the cyber risk and architecting defense layers

This session will deliver a high-level introduction to the core elements of the modern cyber space such as, but not limited to, the different types of cyber-attack, the risks embedded in data breaches, attackers' mindset and characteristics, cyber security governance and procedures, remediation techniques.

Required;

- A Special Report on Cyber-Security – Jul 10 2014 – The Economist
  Part 1: http://www.economist.com/news/special-report/21606416-companies-markets-and-countries-are-increasingly-under-attack-cyber-criminals
- Trautman, Lawrence J. and Altenbaumer-Price, Kara, **The Board's Responsibility for Information Technology Governance** (December 17, 2010). John Marshall Journal of Computer & Information Law, Vol. 29, p. 313, 2011
- *Khalid Kark, Tonie Leatherberry and Debbie McCormack***, Technology and the Boardroom: A CIO's Guide to Engaging the Board,** Harvard Law School Forum on Corporate Governance and Financial Regulation*, **Monday, March 11, 201, Available at:** https://corpgov.law.harvard.edu/2019/03/11/technology-and-the-boardroom-a-cios-guide-to-engaging-the-board/

Academic Literature and additional background (Permission);

- Trautman, Lawrence J., **Threats Escalate: Corporate Information Technology Governance Under Fire** (November 5, 2012).
- Malhotra, Yogesh, **Cybersecurity & Cyber-Finance Risk Management: Strategies, Tactics, Operations, &, Intelligence: Enterprise Risk Management to Model Risk Management: Understanding Vulnerabilities, Threats, & Risk Mitigation** (September 15, 2015).
- Timeline of cyber attacks: https://en.wikipedia.org/wiki/List_of_security_hacking_incidents
- Worlds biggest data breaches http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
- Layered Security: Why it Works – SANS Institute
  https://www.sans.org/reading-room/whitepapers/analyst/layered-security-works-34805

***** Guest Lecture by Menny Barzilay***, Emerging cyber security threats.

Module 2 – The NIST information security framework

A special attention will be given to the NIST CYBER SEUIRTY FRAMEWORK. The class will be introduced to the five functions of the cyber security framework: Identify, Protect, Detect, Respond and Recover. This framework will be used as a common ground to guide all the case studies and discussions given throughout the course.

Required;

- NIST Framework: https://infocus.dellemc.com/michael_dulavitz/strengthen-security-of-your-data-center-with-the-nist-cybersecurity-framework/
- NIST Guide for Conducting Risk Assessments **https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final**

Module 3 - Data-Driven cyber security – towards proactive approach

Required;

- How predictive analytics discovers a data breach before it happens – Jul 25 2016 – TechCrunch https://techcrunch.com/2016/07/25/how-predictive-analytics-discovers-a-data-breach-before-it-happens/
- Using Predictive Analytics to Identify Cyber Security Risks – Feb 17 2016 – Information Management http://www.information-management.com/news/big-data-analytics/using-predictive-analytics-to-identify-cyber-security-risks-10028270-1.html
- Shackelford, Scott J. and Charoen, Danuvasin and Waite, Tristen and Zhang, Nancy, **Rethinking Active Defense: A Comparative Analysis of Proactive Cybersecurity Policymaking** (December 18, 2018). University of Pennsylvania Journal of International Law, 2019.

Academic Literature and additional background (Permission);

- Kello, Lucas, **Private-Sector Cyberweapons: Strategic and Other Consequences** (June 15, 2016).
- Jalali, Mohammad and Kaiser, Jessica**, Cybersecurity in Hospitals: A Systematic, Organizational Perspective** (January 11, 2018). MIT Sloan Research Paper No. 5264-18.
- Smith, McKay and Mulrain, Garrett, **Equi-Failure: The National Security Implications of the Equifax Hack and a Critical Proposal for Reform** (September 1, 2018). Journal of National Security Law & Policy, Vol. 9, No. 3, 2018.
- Carter, William, **Forces Shaping the Cyber Threat Landscape for Financial Institutions** (October 2, 2017). SWIFT Institute Working Paper No. 2016-004.
- Malhotra, Yogesh, **Cybersecurity & Cyber-Finance Risk Management: Strategies, Tactics, Operations, &, Intelligence: Enterprise Risk Management to Model Risk Management: Understanding Vulnerabilities, Threats, & Risk Mitigation**, (September 15, 2015).
- Security Analytics: Big Data Analytics for cybersecurity: A review of trends, techniques and tools http://ieeexplore.ieee.org/document/6725337/

Module 4 – Between privacy and cyber security – strategic approach for privacy policy

Required;

- The EU General Data Protection Regulation**, https://eugdpr.org/**
- O'Brien, David R., Ryan Budish, Rob Faris, Urs Gasser, and TIffany Lin. 2016. **Privacy and Cybersecurity Research Briefing**. Berkman Klein Publication Series, Available at; **http://nrs.harvard.edu/urn-3:HUL.InstRepos:28552575**

**** Guest lecture: Adv. Ido Manor, HFN**

Module 5 - Big data and information sharing in Cyber

Required;

- Federal Cybersecurity Information Sharing Act signed into law – Jan 3 2016 – Norton Rose Fullbright Data Protection Report http://www.dataprotectionreport.com/2016/01/federal-cybersecurity-information-sharing-act-signed-into-law/

- Cyber Threat Information Sharing: Recommendations for Congress and the Administration – Mar 2015 – Center for Strategic & International Studies

https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150310_cyberthreatinfosharing.pdf

- Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace – Apr 1 2014 – Heritage Foundation
  http://www.heritage.org/research/reports/2014/04/cybersecurity-information-sharing-one-step-toward-us-security-prosperity-and-freedom-in-cyberspace

Additional background (Not required);

- Ponemon Institute Big Data Cybersecurity Analytics Research Report
  http://www.cloudera.com/content/dam/www/static/documents/analyst-reports/big-data-cybersecurity-analytics-research-report.pdf

- Big Data: Cyber Security's Silver Bullet? Intel Makes the Case – Nov 9 2014 - Forbes
  http://www.forbes.com/sites/kurtmarko/2014/11/09/big-data-cyber-security/#69768805294e

APPENDIX: CASE STUDIES & SIMULATIONS

Overview

The main objective of the course is to provide executives, directors and managers a high-level overview of various aspects of Cyber security in the context of current threats and characteristic of the cyber domain. The growing interest of practitioners in different "Cyber for the boardroom" methodologies exemplifies the importance of this curriculum. While there is no debut on the tremendous economic effect correlated with cyber events on every modern corporation, directors and managers are know more than ever are obliged by their professionals' duties to set the organizational security framework.

This course aims to leverage the NIST CYBER SEUIRTY FRAMEWORK into practical tools for the course's participants, tools that can describe as crucial to any businessperson operating in the hyperactive treat ordinated digital environment. Through lectures, demonstrations, case studies and group discussions we hope to enable useful insights for the participants. The interactive course will focus on designing a cyber-security framework for the organization, determine and manage the organization's personal cyber risk profile. In addition, the case studies will demonstrate best practices the management should handle in the event of data breach or any other kind of cyber event.

Introduction to cyber security and hot trends in the cyber space, The NIST framework

Required;

- NIST Security dashboards: https://www.tenable.com/blog/understanding-nist-s-cybersecurity-framework
- Significant attacks: https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents
- Attacks on financial institutions: https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline
- Cyber security operationhttps://www.cgi-group.co.uk/en-gb/brochure/cyber-security-threat-vulnerability-and-risk-assessment
- Types of attacks https://pagely.com/blog/cyber-attacks-in-2018/\
- History of Hacking https://medium.com/@marinivezic/the-history-of-cyber-kinetic-attacks-and-incidents-96c787c13f2d
- Cyber statistics https://www.varonis.com/blog/cybersecurity-statistics/
- Examples of cyber attacks in various sectors: https://en.wikipedia.org/wiki/List_of_cyberattacks
- List of data breaches: https://en.wikipedia.org/wiki/List_of_data_breaches

Additional Background

- Timeline of cyber attacks: https://en.wikipedia.org/wiki/List_of_security_hacking_incidents
- common attacks terminology: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html
- The different aspects of cyber loss in incident: https://www.risklens.com/blog/the-six-types-of-loss-in-cyber-incidents/
- Email compromise attack file:///Users/nimrodkozlovski/Downloads/Business_Email_Compromise_Attacks_and_How_to_Protect_Your_Business.pdf

Industry spotlight - the healthcare industry

Cybersecurity incidents are a growing threat to the health care industry in general and hospitals in particular. The health care industry has lagged behind other industries in protecting its main stakeholder (ie, patients), and now hospitals must invest considerable capital and effort in protecting their systems. However, this is easier said than done because hospitals are extraordinarily technology-saturated, complex organizations with high end point complexity, internal politics, and regulatory pressures.

Basic;

- Case study; How unsecured medical record systems and medical devices put patient lives at risk https://www.sciencedaily.com/releases/2018/08/180829115554.htm
- Case study: A Brief Chronology of Medical Device Security, https://cacm.acm.org/magazines/2016/10/207766-a-brief-chronology-of-medical-device-security/fulltext
- Shackelford, Scott J. and Mattioli, Michael and Myers, Steven and Brady, Austin E. and Wang, Ruihan and Wong, Stephanie, **Securing the Internet of Healthcare** (February 22, 2018). Minnesota Journal of Law, Science & Technology, 2018; Kelley School of Business Research Paper No. 18-16.
- Medical devices security: https://www.kaspersky.com/about/press-releases/2016_how-i-hacked-a-hospital-kaspersky-lab-finds-security-weaknesses-in-health-it
- Medical connectivity risk: https://medicalconnectivity.com/2018/01/08/medical-device-security-threat-predictions-for-2018/
- Medical device vulnerability: https://www.databreachtoday.com/medical-device-vulnerability-alert-issued-a-5847

Additional;

- Security Threats in HealthCare Systems, Available at: https://consoltech.com/blog/security-threats-healthcare-systems/
- Cyber Attacks: In the Healthcare Sector, Available at: https://www.cisecurity.org/blog/cyber-attacks-in-the-healthcare-sector
- High demand for medical records in the black market, Available at: https://resources.infosecinstitute.com/category/healthcare-information-security/healthcare-cyber-threat-landscape/top-cyber-security-risks-in-healthcare/#gref
- Live demo: https://ucsdnews.ucsd.edu/pressrelease/how_unsecured_obsolete_medical_record_systems_and_medical_devices_put_patient_lives_at_risk
- Additional live demo (pump manipulation) https://www.youtube.com/watch?v=OpyYLJOLwpA&feature=youtu.be

Industry spotlight - the financial industry – From JP Morgan to Cryptocurrency

Protecting financial networks not only requires financial institutions to improve the security of their own systems, but to change the security balance of the entire internet environment. Cyber threats to financial institutions increasingly come from insecure low-cost mobile and IoT devices outside their own networks. This requires new approaches to defense, including developing new authentication and monitoring technologies for bank networks, and supporting the development of security solutions for these new devices outside the banks' own networks. Improving cybercrime

education and awareness for new internet users in the developing world and supporting efforts to build law enforcement capacity to combat cybercrime around the world is also critical.

Basic;

- Case study: Japanese cryptocurrency exchange loses more than $500 million to hackers, Available at: https://www.cnbc.com/2018/01/26/japanese-cryptocurrency-exchange-loses-more-than-500-million-to-hackers.html
- Case study: Crypto Website Coinmama Hacked, Data on 450,000 Users Stolen, Available at: https://www.calcalistech.com/ctech/articles/0,7340,L-3756485,00.html
- Case study: Was Capital One hacked or breached? How did it happened and who is to blame?, Available at: https://www.newsweek.com/capital-one-hack-breach-cybersecurity-paige-thompson-amazon-web-services-what-data-exposed-1451734?amp=1
- Craig A. Newman and Maren J. Messing, Patterson Belknap Webb & Tyler LLP, **Bull or Bear? How the Market Reacts to Data Breach**, Harvard Law School Forum on Corporate Governance and Financial Regulation, Tuesday, November 20, 2018, Available at: https://corpgov.law.harvard.edu/2018/11/20/bull-or-bear-how-the-market-reacts-to-data-breach-news/
- Malhotra, Yogesh, **CyberFinance: Why Cybersecurity Risk Analytics Must Evolve to Survive 90% of Emerging Cyber Financial Threats, and, What You Can Do About It? Advancing Beyond 'Predictive' to 'Anticipatory' Risk Analytics** (June 8, 2016). Research Presentation at the 19th New York State Cyber Security Conference Presentation, Albany, NY, June 8-9, 2016, Empire State Plaza, Albany, NY.
- Guide to Cybersecurity for Financial Services Firms, best practices summary for the financial industry; Available at : http://www.cutoday.info/content/download/26039/218761/version/1/file/Lockheed+Martin+Guide+to+Cybersecurity.pdf

Additional;

- Craig A. Newman, Patterson Belknap Webb & Tyler LLP, SEC Cyber Briefing: Regulatory Expectations for 2019, Harvard Law School Forum on Corporate Governance and Financial Regulation, *Wednesday, January 2, 2019,* Available at: https://corpgov.law.harvard.edu/2019/01/02/sec-cyber-briefing-regulatory-expectations-for-2019/
- *Khalid Kark, Tonie Leatherberry and Debbie McCormack***, Technology and the Boardroom: A CIO's Guide to Engaging the Board,** Harvard Law School Forum on Corporate Governance and Financial Regulation*, **Monday, March 11, 201, Available at:*** https://corpgov.law.harvard.edu/2019/03/11/technology-and-the-boardroom-a-cios-guide-to-engaging-the-board/

Case Studies (General reading items):

- Case study: Wired Jeep hack demo: https://www.youtube.com/watch?v=MK0SrxBC1xs
- Case study: Demo of mobile phone hack (Man in the middle wifi attack and malicous network): simulation of phishing, media disinformation https://www.youtube.com/watch?v=dysnKiXUlRU&t=924s
- Case study: Ransomware attacks explained (video): https://www.pbs.org/newshour/show/ransomware-attack-takes-down-la-hospital-for-hours
- Austrian hotel door hack: https://www.wired.co.uk/article/austria-hotel-ransomware-true-doors-lock-hackers

- Baby Monitor Hack: https://www.cnn.com/videos/us/2018/12/19/baby-monitor-hacked-threat-houston-vpx.hln
- Email business fraud: https://www.forbes.com/sites/kerrizane/2018/04/16/the-shocking-new-scam-you-need-to-know-about-money-transfers/#86f6c351c56c