BUS 281f
Cyber security and operational risks
Fall 2018

Mondays, 6:30 pm – 9:20pm

Professor Erich Schumann
eschumann@globalatlanticpartners.com

Course pack: https://hbsp.harvard.edu/import/583109

OVERVIEW

There is no security in this world; only opportunity (Douglas McArthur)
A good decision is based on knowledge and not on numbers (Plato)

Both phrases retain its meanings even more in today's environment. Organizations are facing amazing technological developments, instantaneous communications, globally distributed customer bases and workforce, and lean and modularized supply chains. It has become more difficult to manage, that is, identify, assess, prioritize, mitigate and monitor potential risks. The reality of this brave new world is that risk is on the rise, threats have become more pervasive and vulnerabilities more relevant. In addition to traditional risks, such as liquidity, market and operational risks, cyber risks are moving up in the ranks of relevant risks. There are two questions which managers need to ask: 1. How much and what type of risk do we have? 2. What do I need to do to mitigate risks to an acceptable level? To be effective, today's managers must be able to assess the risk profile of their businesses and respond to issues as they arise. **The cyber security industry in the United States faces a massive problem: there are simply not enough highly-skilled cyber security professionals. This is already a massive issue, but fast-forward to 2020 and the shortfall is expected to reach 1.5 million (and many more globally).**

In this course, we examine how companies:

- use the Enterprise Risk Management - integrated framework from COSO (Committee of Sponsoring Organizations of the Treadway Commission), NIST, ISO and ISACA (Information Systems Audit and Control Association),
- prepare to detect, prevent and recover from a cyber-attack; for any company it's not a question if they will experience an attack but when the attack will happen, and how much it will take to recover from the attack
- should build "risk intelligent" organizations with the goal to create and preserve value and survive and thrive in uncertainty

Learning goals:

The exit level outcomes of this course will be:

- ✓ Show how cyber and other risk management mitigates business risks within the desired risk appetite
- ✓ Investigate the threats to an organizations critical business processes
- ✓ Assess the vulnerabilities to an organization's strategic relevant business activities incl. critical business systems, technology and data
- ✓ Distinguish the legal and compliance risks for an organization
- ✓ Propose an incident response plan to prepare an organization in the event of a cyber attack

COURSE REQUIREMENTS

Required Readings (available through the bookstore and by hand-outs during the course)

- A course packet consisting of business school cases, notes, and articles
- Governance & Risk from Standard & Poor's (selected pages)
- Measuring and managing information risk (selected pages)
- Implementing the NIST cybersecurity framework (selected pages)
- Enterprise Risk Management handbooks

Prerequisites

Students need to be able to read and understand a company's financial statements. As such, students are expected to have a familiarity with accounting.

Class Participation

Lively class participation is expected of everyone in this course, and class attendance is required. Each week, there will be a business case or note assigned and every student is expected to be prepared to discuss it in detail.

Homework (one written analyses)

The analysis, to be done individually, is due at the start of class 4. Specific topics will be assigned during the course. The analysis is worth 25% of the final grade. The analyses are typically 3 - 4 pages in length.

Final Paper

The final paper (8 to 10 pages + exhibits) is intended to reflect the students' knowledge and judgment on Enterprise Risk Management. Students will be expected to examine the issue from the perspective of senior management. The students can choose any type of company (privately owned which intends to go public), small or medium sized, etc., as long as it addresses one or more of the major issues raised in the course, analyzes a real company, and includes recommendations directed to the company's management.

Grading

Final Paper	40%
Homework (individual analysis)	25%
Class Participation	25%
Multiple choice test	*10%*

Office Hours

Students can meet with me after class or by appointment in my office in downtown Boston. To arrange for a meeting, please send me an email at eschumann@globalatlanticpartners.com.

Academic Honesty

You are expected to be honest in all your academic work. The University policy on academic honesty is distributed annually as section 5 of the Rights and Responsibilities handbook. Instances of alleged dishonesty will be forwarded to the Office of Campus Life for possible referral to the Student Judicial System. Potential sanctions include failure in the course and suspension from the University. If you have any questions about my expectations, please ask.

Special Accommodation

If you are a student with a documented disability on record at Brandeis and wish to have a reasonable accommodation made for you in this class, please see me immediately. Please keep in mind that reasonable accommodations are not provided retroactively.

Class I – Identifying and understanding different categories of risk

Competing in any industry entails risk. In this class we consider the different types of risk that can imperil a company. Students will simulate a real life situation and learn how to apply knowledge of the process for analyzing, planning and implementing risk management strategies. We will illustrate how to use the risk matrix – a diagnostic tool to identify organizational pressure points that could cause these risks to rise to dangerous levels. Finally students will be introduced to the NIST and other frameworks related to cyber risk.

Required Reading

History or Risk Management: History, Definition, and Critique – will be distributed before class
An Overview of Risk and Risk Management – **Ivey W 11080**
Sarbanes Oxley Act 2002 – Section 300 and Section 400
NIST Cyber framework – will be distributed before class

Class II – Relevant risk frameworks and its implementation

In this class we will study in detail the operational framework COSO and the technology control framework COBIT. We will discuss the roles of management, risk professionals and audit department (three/four lines of defense model). We will use practical examples of real life companies who implemented both frameworks. At the end of the classes the students will be able to identify risks and controls for specific processes using these frameworks.

Required Reading

Enterprise Risk Management – Integrated Framework from the Committee of Sponsoring Organizations of the Treadway Commission (COSO) – will be distributed before class
Risk Appetite and Tolerance, qincluding definition of Cyber risk appetite. Guidance Paper by IRM – will be distributed before class
How continuous monitoring is revolutionizing risk management and how technology is assisting – will be distributed before class

Class III – Importance of Risk Management

Risk recognition and risk rating together form the risk assessment component of the risk management process. Risk assessment involves the recognition of risks and the rating of them to determine the significant risks facing the organization, project or strategy. We will analyze the Target data breach. This case revisits the events in late 2013 that gave rise to what was at the time the largest breach of confidential data in history. The case presents the cybercriminals' activities leading up to the breach, details of the commission of the theft, the measures that Target had put in place to deter such attacks, its ill-fated response during the attack and, finally, the impact of the breach on Target as well as on the retail industry as a whole.

Required Reading

Fundamentals of Risk Management by Paul Hopkin - reprints of the relevant pages will be provided
Measuring and managing information risks – reprints of the relevant pages will be provided
Autopsy of a data breach – The Target case **HEC 130**

Class IV – Realizing Business Value and Managing Cyber Risk

NOTE: HW Assignment #1 is due at the start of class

Managing Cyber risk is a major challenge for management; frameworks, such as NIST or ISO 27000 are useful tools, however, successful implementation requires clearly defined proactive strategies. Students will learn relevant steps to detect, recover, mitigate, respond to incidents and prevent cyber risk. During class we will analyze the Sony data breach and show management failed in preventing a major data leak. Students will learn about various cyber threats and the dark net as market place for stolen data.

Required Reading
They burned the house down – Sony case **Reprint R1507J**
The Vulnerability economy **KS 1013**

Class V – Enterprise Risk Management report and Risk Dashboard

The purpose of this class is to understand how to implement ERM and use the Balanced Scorecard approach to prepare a risk dashboard can help companies to improve risk management and governance. We will discuss the failure of risk management process in a company and will analyze if the implementation of a risk dashboard would have helped to avoid wrongdoing. At the end of the class the students will be asked to opine on the pros and cons of implementing a risk dashboard.

Required Reading

Balanced Scorecard concept - will be distributed before class
Enterprise Risk Management at Hydro One **5-110-086**

Class VI – IT Management Cyber attack simulation

For any company the risk of experiencing a data breach and other risks is real, it's not a question of "if" but "when it will happen". Companies must be prepared how to respond in case the event happens. Students will learn about an "real life" event and are asked to develop an incident response based on information provided during class.

Required Reading

Strategies for incident response and cyber crisis – will be distributed before class