Risk Management in Information Technology
INFO GB 3351
INFO UB 0051
Preliminary Fall 2017

Instructor: Bernard S. Donefer
E-mail: bdonefer@stern.nyu.edu
Website: http://pages.stern.nyu.edu/~bdonefer/
Class Times: Thursday 6:00 – 9:00 p.m. Room TBD
Office Hours: Thursday 4:00-5:00 p.m., KMC 8-171 or after class or by appointment
Class-site: NYU Classes – all announcements, assignments, readings and class notes

Background

The national and economic security of the U.S. and all nations depend on the reliable functioning of critical infrastructure. This includes financial, communications, power, health and essential systems and services relying on information technology. Recent events demonstrate that governments, businesses and individuals are vulnerable to attack from external adversaries, as well as self-inflicted difficulties. Intellectual property can be stolen, customers’ privacy violated and operations disrupted. Such events drive up costs, reduce revenue, impact innovation and cause reputational damage.

To better address these risks, President Obama issued Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” on February 12, 2013, which established that “[i]t is the Policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.”

Course Objectives

This course will address the issues faced by management responsible for ensuring the security of organizational technology, communications and data infrastructure. These typically fall under the purview of the chief information officer (CIO). It will address topics in operational risk, project management, cybersecurity, disaster recovery and protecting intellectual property. We will use cases and examples sourced from news and real life illustrations from guest lecturers across industries such as banking, securities, health and hospitals, retailing, utilities, etc.

We will focus on compliance with commonly accepted best practices and regulatory requirements. These will include guidelines of the National Institute of Standards and Technology (NIST), Homeland Security - Cybersecurity recommendations and industry specific regulations from the Securities and Exchange Commission (SEC), Health and Human Services (HHS) and similar regulatory bodies.
There will be a project requirement, where teams of four students create a security plan for an organization in the industry of their choice. It will be presented to the class at our last class session.  *(Note: Project may be in lieu of a final exam and reflect in grading.)*

**Prerequisites – Course Audience**

There are no required prerequisites for this course. However, to successfully understand the material, you should have a general understanding of technology, communications and the internet and their management. This is not a programming or technical course but geared to students aiming for “C” roles where their firm’s technology is critical to its success. It can be taken by technologists, senior managers in finance, administration, risk or general management, compliance officers, auditors, regulators and anyone who needs a broad introduction to the topic.

**Primary Text and Readings**

There is no text for this course. There will be both readings and cases that will be provided on NYU Classes for each topic in the syllabus. All class notes and readings will be posted to the class NYU Classes website prior to each class.

**Methodology**

The class will be based on lectures, readings, case studies and guest speakers. Besides a mid-term and final exam, students will prepare an assignment based on an assigned case.

**GRADING**

<table>
<thead>
<tr>
<th>Item</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Midterm</td>
<td>35%</td>
</tr>
<tr>
<td>Project</td>
<td>20%</td>
</tr>
<tr>
<td>Final</td>
<td>35%</td>
</tr>
<tr>
<td>Class Participation</td>
<td>10%</td>
</tr>
</tbody>
</table>

**Default Policies for Stern Courses**

**Laptops, Cell Phones, Smartphones, Recorders & Other Electronic Devices**

May not be used in class. **You must TURN OFF all devices BEFORE class. If your phone rings, you will be asked to leave.** Further I reserve the right to reduce your final grade by reducing points normally awarded for class participation. If you are on-call for work or family, just place your device on vibrate and leave the room before taking the call.

**Attendance**

Required and part of grade.

Faculty will excuse absences and entertain requests to change exam and assignment due dates only in cases of documented serious illness, family emergency, religious observance, or civic obligation. If you will miss class for religious observance or civic obligation, you must inform your instructor no later than the first week of class. Recruiting activities, business trips, vacation travel, and club activities are not acceptable reasons for absences or requests to reschedule exams and assignments.

**Arriving Late, Leaving Early, Coming & Going**

Arriving late interferes with other students' learning and is not acceptable. Subway delays and other problems are unavoidable on occasion, but it is each student's responsibility to plan carefully to arrive
on time and well prepared. Repeated latecomers will be penalized. Students are expected to arrive to class on time and stay to the end of the class period.

Arriving late or leaving class early may impact the course grade. Students may enter class late only if given permission by the instructor and can do so without disrupting the class. (Note that instructors are not obliged to admit late students or readmit students who leave class.)

**Late Submission of Assignments**

Late assignments will incur a grade penalty unless due to documented serious illness or family emergency. Instructors will make exceptions to this policy for reasons of religious observance or civic obligation only when the assignment cannot reasonably be completed prior to the due date and the student makes arrangements for late submission with the instructor in advance.

**General Behavior**

You may eat in class as long as it is not odiferous or noisy. There will be a break at about 7:30 when you can get “dinner”. Please clean up and throw away all trash.

As a mark of respect, I ask all men to remove their caps or hats while in class, unless worn for a religious reason.

Students will conduct themselves with respect and professionalism toward faculty, students, and others present in class and will follow the rules laid down by the instructor for classroom behavior. Students who fail to do so may be asked to leave the classroom. (NYU Stern Code of Conduct) For more information on NYU Stern's Code of Conduct for current students, please log in [here](https://www.stern.nyu.edu/policies/code-of-conduct).

**Disability**

If you have a qualified disability and will require academic accommodation during this course, please contact the Moses Center for Students with Disabilities (CSD, 998-4980) and provide me with a letter from them verifying your registration and outlining the accommodations they recommend. If you will need to take an exam at the CSD, you must submit a completed Exam Accommodations Form to them at least one week prior to the scheduled exam time to be guaranteed accommodation.

**Your e-mail address**

Be sure your email address in NYU Classes is correct. I will use it to communicate timely information about the course. To update your e-mail address in NYU Classes, log into NYU Home at [https://home.nyu.edu/](https://home.nyu.edu/) Click Preferences at the top of the screen and then edit your Directory Address, which will be reflected in NYU Classes within 24 hours.

**Collaboration on Graded Assignments**

Students may not work together on graded assignment unless the instructor gives express permission. (NYU Stern Code of Conduct) For more information on NYU Stern's Code of Conduct for current students, please log in [here](https://www.stern.nyu.edu/policies/code-of-conduct).

**Grading**

MBA students who do not submit Course Faculty Evaluations by the deadline will not have access to their final grades until the grade release date, which is determined by program. Faculty are requested not to release final grades to students who fail to submit evaluations and students should not ask. (Stern policy)

**Recording Classes**

At any time, your classes may be recorded for educational purposes. (Stern policy)
Syllabus
(Schedule Subject to Change – Refer to NYU Classes)

(Dates and Readings will be added before being finalized)

1. Background
   a. How security supports the business mission
   b. Economics of good risk management
   c. Constituencies of clients, employees, shareholders and management
   d. Societal issues and expectations

2. Governance
   a. Organization of risk responsibilities
   b. Senior management and board of directors
   c. Chief risk and information security officers
   d. Auditors and regulators
   e. Integration of business and IT management
   f. Policies

3. Operational risk – identification and prioritization
   a. Control self-assessments
   b. Key risk indicators and action plans
   c. Prioritization, likelihood vs impact
   d. Op risk reporting systems
   e. Operational improvement, Six Sigma, TQM

4. Regulatory directives
   a. Homeland Security
   b. NIST Framework
   c. FFEIC, SEC Reg SCI, HHS, etc.

5. Data security and privacy – examples of recent breaches and their impact
   a. Threats and vulnerabilities
      i. Internal vs. external
   b. Hackers, from script kiddies to foreign espionage
6. Cybersecurity
   a. Asset identification -- what data, resources and processes are at risk
   b. Attack surface – vulnerable access points
   c. Threat identification and protection measures
   d. Detection, recovery and disclosure

7. Access controls
   a. Multifactor
   b. Biometrics
   c. Smart chip technology
   d. Remote access, VPNs
   e. Securing the cloud
   f. Media controls, physical access

8. On-line security
   a. Social engineering and training
   b. Phishing, pharming and email attacks
   c. Malware, ransomware
   d. Denial of service attacks
   e. TLS, cryptography and digital signatures
   f. Techniques used in blockchain

9. Disaster preparation and recovery
   a. Backing up
      a. Cloud based backup and risks
   b. Applications, network, staffing
   c. Power, communication, critical resources
   d. Contingency planning
   e. Hurricane Sandy, WTC 1993 attack and similar cases

10. IT project management risks
   a. Incorporating risk mitigation in software design

11. Intellectual property – protecting system business processes
   a. Patents and copyright
      a. When and how to use
   b. Protection
   c. Infringement