Risk Management in Information Technology
INFO GB 3351
INFO UB 0051
Fall 2019 - *Preliminary*

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 KMC 4-80
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 cases 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.

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 (TCP/IP) 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, 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 required text for this course. Both readings and cases, as well as class notes will be provided on NYU Classes for each topic in the syllabus prior to each class.

I am sometimes asked for additional textbook sources. You might find these two books of interest. However, **I will not refer** to them during our course and they are only two of dozens of books on the subject. I have not requested them to be ordered by the NYU Bookstore, but they are available on Amazon. **They need not be purchased for this class.**

Computer Security: Principles and Practice, 4th Ed. by William Stallings, Lawrie Brown
Effective Cybersecurity: A Guide to Using Best Practices and Standards 1st Ed by William Stallings

Recording Classes and Email

All classes are recorded and will be available to you on NYU Classes.

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/ . Click Preferences at the top of the screen and then edit your Directory Address, which will be reflected in NYU Classes within 24 hours.

Methodology and Grading

The class will be based on lectures, readings, case studies and guest speakers. There will be a mid-term and final exam and a cyber-attack analysis project. Note the importance of class participation. It represents a half a grade level in your final ranking.

Item	*Grade*
Midterm	35%
Project (optional)	20%
Final	35%
Class Participation	10%

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)

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.

I 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 me 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.)

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).

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.

Syllabus
(Schedule will be announced in class)

Part I -- Risk Management in Information Technology

1. IT risk ***is*** business risk
    a. Examples of IT failures
        i. Constituencies of clients, employees, shareholders and management
    b. What is risk?
    c. How security supports the business mission
    d. Governance
        i. Tiered organizations, boards, senior management, etc.
    e. Corporate standards on financial reporting
    f. Privacy and public expectations
    g. Economics issues in IT risk management
        i. Security metrics
    h. Are business goals met by IT efforts
2. Information technology management
    a. CIO
        i. Next generation of risks
    b. CRO
    c. CISO
        i. Levels of data
    d. Risk strategy and organization
    e. Self-audits
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. Business continuity and disaster recovery
    a. Backing up
        i. 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 events
5. Standards, Directives and Framework
    a. Homeland Security
    b. NIST Framework
    c. Regulations
        i. FFEIC, SEC Reg SCI, HHS (HIPAA), etc.

Part II – Cybersecurity

6. On-line security and Cryptography
    a. Cryptography
    b. Hashing
    c. Internet security SSL/TLS and certificate authorities
    d. Digital signatures
7. Introduction to 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. The Target and Home Depot Hacking Cases
8. Authentication and access control
    a. Multifactor
    b. Biometrics
    c. Smart chip technology
    d. Remote access, VPNs
    e. Media controls, physical access
    f. The Equifax Hacking Case

Cyber Attack Harvard Simulation in Class and post sim analysis

9. Review of communications
    a. TCP/IP and UDP
    b. Routers, Switches
    c. VPNs
    d. Ports
    e. Firewalls
10. Cloud computing
    a. Suitability
    b. Deployment and service models
    c. Micro-segmentation and containerization
    d. Mobile devices and IOT
11. Cyber kill chain
    a. Advanced persistent threats (APT) model
    b. Seven steps, attacker and defender roles and actions
    c. Use of cyber kill chain methodology to organize defensive strategies
12. Introduction to penetration testing or how do hackers do it
    a. Hackers, from script kiddies to foreign espionage
    b. Review Cert vulnerability alerts https://www.us-cert.gov/ncas/alerts
    c. Setting up virtual machine penetration testing environment
    d. Using Kali Linux platform examine techniques used by hackers
    e. Google hacking and reconnaissance
    d. Network address finding and closing vulnerabilities
    e. Review Kali tools available for identifying vulnerabilities