Syllabus

Course	***INFO-GB.2114.20*** ***Introduction to Cybersecurity and Privacy Management***
Schedule	Tuesdays & Thursdays Time: 3:00 pm – 4:20 pm Class Start Date: 3/22/18 Class End Date: 5/01/18 + Final Project simulation during exam week Date: TBD
Instructor	Gary Podorowsky
Contact Information	Gary.Podorowsky@gmail.com
Course Summary and Learning Objectives	This course will introduce students to the key issues in cybersecurity and privacy management and help them to develop a basic understanding of business, technical, legal and ethical issues related to cybersecurity and privacy. At the end of the course, the students will understand the set of common cybersecurity and privacy-related business challenges faced by managers. They will learn how managers cope with these challenges across different industries by developing robust Information Security and Privacy Management Programs to maintain confidentiality, integrity and availability of the information, networks, computing systems and applications managed by the organization. After developing a basic understanding of the key topics covered in the class, the students will be prepared to have incisive conversations with cybersecurity and privacy experts and be able to ask pertinent questions on a wide range of cybersecurity and privacy topics. Examples of issues to be addressed in this course: ➢ The roles of the Board of Directors and top management in cybersecurity and privacy protection. ➢ How cybersecurity and privacy risks should be incorporated into business decisions. ➢ Cybersecurity and privacy considerations in M&A. ➢ Strategies to prevent intrusions and theft of data and to detect intrusions if they do occur. ➢ How to prepare for the advent of a data breach, and necessary actions following a breach, with a focus on critical business decisions that senior corporate management will face. ➢ Unique privacy management requirements for marketers, for the financial industry and for the healthcare industry, as well as workplace privacy issues across industries. ➢ Cybersecurity and privacy considerations with respect to the Internet of Things (IoT). This course features lectures, practitioner guest lecture(s), discussion and analysis of real world examples/case studies, and a cybersecurity crisis-response simulation project.

Class #s and Dates			Topic	Sub-topics		Notes

Course Prerequisites	**None**
Materials/Books	**Supplied by Instructor:** Handouts, including cases, exercises and articles, as well as some cybersecurity technology backgrounders **Supplied by Student:** 1. ***Cybersecurity for Executives: A Practical Guide****;* Gregory J. Touhill, C. Joseph Touhill; Wiley, 2014 2. ***Privacy Program Management: Tools for Managing Privacy within Your Organization***; Russell R. Densmore, Executive Editor; International Association of Privacy Professionals; 2013 3. ***(Possible Supplemental Text (TBD))*** (Syllabus continues on next page)

Class #s and Dates			Topic	Sub-topics		Notes
Classes 1 & 2 **3/22 and 3/27**			**The Mission and Landscape of Cybersecurity Management and Privacy Management**	• Objectives of cybersecurity and privacy management • Historical and global context, including significant recent breaches (e.g., Equifax, HBO, Yahoo!, Target, Anthem) and their consequences • Types of threat actors (e.g., cyber-criminals, government-sponsored hackers, etc.) and their objectives • Legal, reputational and other business risks • The increasing importance of cybersecurity and privacy management • Types and examples of business challenges related to cybersecurity and privacy • The roles of the Board and top management in cybersecurity and privacy protection • Fundamental differences in regional approaches to privacy protection (e.g., US vs. EU, including reference to the new European Global Data Protection Regulation)		**<u>Case Study</u>** Yahoo's corporate decisions that made it vulnerable to a) breaches b) slow detection of breaches **Homework <u>Assignment</u>** How should cybersecurity and privacy risks be incorporated into business decisions? Who owns these risks? **<u>Readings</u>** To be assigned

Class #s and Dates			Topic	Sub-topics		Notes
Classes 3 & 4 **3/29 and 4/3**			**Key Components of an Effective Cybersecurity and Privacy Management Program**	• Monitor, understand and comply with all applicable laws and regulations • Develop an information governance strategy • Establish, maintain, implement and enforce policies • Communicate with, and ensure buy-in of, top management and the Board of Directors • Take a risk-based approach to cybersecurity and privacy that is consistent with the company's overall enterprise risk program to accept, avoid, mitigate or transfer risks • Help the business to accomplish its goals, while ensuring that cybersecurity and privacy risks do not exceed acceptable levels • Review new collection and use and/or disclosure of personal information, and new vendors and business partners • Maintain detailed inventory of information assets, classified by level of confidentiality and type of information • Train employees, vendors and business partners on cybersecurity and privacy policies and procedures • Prepare for, identify and respond to breaches • Ensure that compliance with all applicable laws, regulations and company policies is audited periodically and that all significant issues are remediated on a timely basis		**<u>Case Study</u>** Re: The $350 million reduction in the price Verizon paid to acquire Yahoo! --- due to the breaches **Homework <u>Assignment</u>** Related to Cybersecurity and Privacy considerations in M&A **<u>Readings</u>** Related to "Accomplish-ing business goals while keeping cybersecurity and privacy risks at acceptable levels," "Defense in Depth" and "Privacy by Design"

Class #s and Dates			Topic	Sub-topics		Notes
Classes 5 & 6 **4/5 and 4/10**			**Building a Robust Risk-based Information Security Management Program (ISMS) to maintain the Confidentiality, Integrity and Availability (CIA) of the information, networks, computing systems and applications managed by the company and its agents** **Strategies to prevent intrusions and theft of data and to detect intrusions if they do occur**	Building a robust Information Security Management Program, including the following components: *(What a businessperson needs to understand about each)*: • Threat Management • Vulnerability Management (incl. remediation (e.g., patching)) • Data Lifecycle Management • Cybersecurity Policies based on a management framework such the ISO or NIST models • Security Operations ○ Monitor, analyze, and manage events and incidents • Cyber-Risk Management • Access Control Management • Network and Cloud Security Management • Host, Data and Application Security • Secure Development • Establishing and maintaining cybersecurity and privacy performance metrics • Mobile Device Management • Use of key cybersecurity tools • Working with vendors and business partners		**Cyber-security Practitioner Guest Speaker** in 4/10 class (including Q&A) (tentative schedule) **Case Study** Re: Manage-ment challenges in developing a corporate cyber-security program **Readings** To be assigned

Class #s and Dates			Topic	Sub-topics		Notes
Classes 7 and 8 **4/12 and 4/17** **Quiz at the start of class on 4/12**			**Quiz** **Data Breaches, Crisis Management, and Business Continuity Planning**	Quiz (40 minutes) on the topics covered in the first half of this course Preparing for, identifying and responding to breaches of personal information • Relationships that should be in place in advance of any serious breach (e.g., forensic investigators, breach legal expert, cyber insurance, cyber-crisis public relations expert, identity theft protection service provider) • Technical actions that must be taken swiftly to contain the breach and verify the safety of the company's networks, systems, computing devices, etc. • Actions that must be taken to achieve a rapid and effective response after learning of a possible significant breach of personal information (e.g., time-sensitive legal notifications (where required), issuance of first statement to public, actions to continue or restore business operations, etc.) • Determinations and decisions needed to make a Rapid and Effective Response (e.g., level of certainty that data was breached, identification of what data was breached and what was not, analysis of legal reporting requirements for notification of this breach, etc.) • Business Continuity in the context of cybersecurity (e.g., determining in advance each business' allowable downtime after a crisis event, back-up systems and applications, activating "hot roll-overs", determining which systems are safe to use, etc.)		**<u>Case Study</u>** Equifax Breach: What mistakes were made? What best practices were not followed? How could following best practices have prevented or mitigated problems at each stage? **<u>Homework Assignment</u>** Analyze the economic/ business impact of the breach on the individuals whose personal information was stolen, and on Equifax

Class #s and Dates			Topic	Sub-topics		Notes
Classes 9 & 10 **4/19 and 4/24**			**Privacy in Marketing;** **Privacy in the Financial Industry;** **Privacy in the Healthcare Industry;** **Workplace Privacy Issues** **Assignment of Final Project**	• Complying with CANSPAM, COPPA and Do Not Call Registry requirements while achieving marketing objectives • *Addressing Fair Credit Reporting Act, FACTA, Gramm-Leach-Bliley Act, Payment Card Industry (PCI), Dodd-Frank and other financial sector privacy requirements* • *Addressing the HIPAA Privacy Rule, the Genetic Information Non-discrimination Act and other healthcare information privacy requirements* • *Workplace Privacy issues, including: protecting sensitive HR data, pre-hire background screening, monitoring of employee activities, handling employee investigations, employee use of personal devices (e.g., mobile phones) for business purposes* <u>Assignment of Final Project</u> In groups of [3], students in the role of the company's senior management will prepare proposed action plans to address a multi-pronged cyber-attack that results in (a) the theft of important intellectual property owned by the company, (b) the theft and public disclosure of sensitive customer personal information, and (c) the company's inability to access an important computer system and stored data unless the company pays ransom to the ransomware perpetrators. The proposed action plans from each group will be due on the first day of Final Exam Week (specific date TBD). See "Session during Final Exam Week" for the second part of this project.		**Reading <u>Assignment</u>** Related to the four topics for these sessions

Class #s and Dates			Topic	Sub-topics		Notes
Classes 11 & 12 ***4/26 and 5/1***			**Business Issues with Significant Cybersecurity and/or Privacy Implications**	Discussion of 4-5 business issues such as: • Determining the amount of resources to allocate to cybersecurity management and to privacy management • Determining the reporting structure of the cybersecurity and privacy management teams to achieve maximum effectiveness • Determining how best to balance marketing business needs, such as collection and processing of consumer personal information, with the maintenance of acceptable cybersecurity and privacy risk levels. • Ensuring compliance by all employees, third-party agents, and business partners with applicable policies, laws, and regulations • Measuring the effectiveness of the company's cybersecurity and privacy management programs • If the programs are best-of-class, determining whether/how this status can be used as a competitive advantage • How to assess the business risks of a hacking of a company's advanced AI-capable products, such as a self-driving car • Considering the ethical, legal, and business implications of screening out job candidates based on content on their social media sites • How to incorporate cybersecurity and privacy into the company's business strategies		
Session during Final Exam Week (Date TBD)			**Final Project Simulation**	We will run a simulation of a realistic post-breach scenario that incorporates the proposed breach management plans the students have submitted. Students will propose follow-on measures as events occur during the simulation.		**Possible Guest** Crisis Mgmt/ Business Continuity/ Privacy/ Cyber-security Programs Practitioner

Class #s and Dates			Topic	Sub-topics		Notes

Grading Criteria	**Class Participation 20%** **Homework 20%** **Mid-term Quiz 25%** **Final Project 35%** **-- Written Submission (20%)** **-- Simulation (15%)**