You have probably heard many times that information security is not just about technology. This course will complement your technical understanding with some key economics, policy and managerial frameworks that explain key challenges in security and privacy for individuals, firms and the nation. For example, we will examine questions like: should a firm be allowed to collect customer information? Would it invest enough in protecting the security and accuracy of this data? Should users and firms be allowed to buy and sell vulnerabilities? Should firms share cyber incident information with government and how? We will analyze these questions within specific economic and policy principles and examine why individuals, firms and governments do not do the “right” thing. Though various practical examples, the course will highlight how interdependencies between different stakeholders, externalities (how one’s actions affects the other stakeholder) and market structure (whether the firm has market power or not) can lead to market failure within the context of information security and privacy.

We will then debate how various policy and economic tools can be applied to mitigate some of these problems. In particular, we will examine product liability (with a focus on software products) laws, cyber-insurance, data breach notification laws, and regulating minimum security requirements. By the end of the course, students are expected to know key managerial and policy issues surrounding information security and privacy provision, the role of policy and economics tools in engendering desired outcomes, and the limitations and challenges of such interventions.

The course will feature multiple guest speakers from industry practitioners, and case studies as part of instructions. There is no text book and all reading material will be provided on the first day of class. Some understanding of economics is expected.

**Syllabus**

All reading material can be accessed via class blackboard.

**Week 1:** Introduction and Role of Market and Competition in providing security and privacy.

We will start with the discussion on the current level of security provision by vendors and security adoption by users. The goal is to understand how market structure (like competition and monopoly) affect the level of security privacy.
**Week 2: Externalities and Market Failures**

Externalities are considered a major cause of market failure for security. Externalities mean the action of one party has consequence for another party. We will consider various forms of externalities in the context of information security. Some externalities are related to coordination problems, while others purely cause congestions. We will investigate them in the context of “Spam” and deployment of Security Technologies, information sharing and so on.

**Week 3: Policy tools**

We will examine what policy tools can be employed to overcome externalities and efficacies of these tools under different scenarios. We will consider subsidies, tax, mandated standards, regulations and liability amongst many such options. We will consider the role of assigning property rights and liability as policy tools. In particular, we will develop a framework to examine when policy interventions may (or may not) make sense.

**Week 4: Data Breach Notification and Other policies**

We will go over specific security and privacy related policies and their impact via a case study (ChoicePoint)

**Week 4: Cyber-insurance**

One of the ways risks are mitigated in via insurance. We will spend some time on understanding the key principles behind cyberinsurance. More importantly, we will discuss some of the problems in development of such a market. We will go over what policies are offered, what are excluded, what is the market size etc.

**Week 5: Direct and Indirect liability**

In this module, we will focus in the current state of law making regarding product liability and how those apply to software quality and security. In particular, we will focus on what the key responsibilities of software vendors are regarding their product and how/why it differs from other goods.

**Week 6: Zero Day Vulnerabilities.**

I will start our discussion on challenges of disclosing information (vulnerability disclosure). We will start with what is vulnerability disclosure, key stakeholders in disclosure, and key issues surrounding disclosure. We will then discuss the problem of zero vulnerabilities, their buying and selling in black market as well as to the government agencies.
Week 7: Summarization, Wrap up and Final exam review