Information Security and Privacy

Course Title	Information Security and Privacy
Instructor(s)	Prof M P Sebastian
Course credit	3
Total No. of Sessions	27
Session Duration	60 minutes
Term	
Year	2012-13

Introduction:
Information security has become mandatory for business to perform their day-to-day functions efficiently. Given the crucial role played by information systems, it is important that they remain secured and that the data contained in them do not fall into the hands of those who are not intended to have access to it. Preservation of the integrity of electronically generated documents and their authentication are vital for e-business.

Course Objectives:

The objective of this course is to introduce the theory and practice of information security management, and to examine the business and managerial challenges involved in it. The scope of this course include the basics of security, Physical and Environmental Security, Network Security and Logical Access Control, Models, Frameworks and Metrics for Security, Privacy – Business Challenges and Technological Impacts, and Security Best Practices. The participants can plan for an information security management strategy for an organization.

Prerequisite:
The course does presume some level of familiarity with computer and Internet technologies.

Course Contents:

Threats to information systems, Cyber offences and identity theft, Security life cycle, Building blocks of security, Risk analysis, Mathematical foundations of security, Symmetric key cryptography, Public key cryptography, Message authentication, Digital signature, Physical and perimeter security, Biometrics, Network security, Intrusion detection and firewalls, Wireless and mobile security, Email security, Security of databases and OS, Security models and standards, SSE-CMM, Security metrics, Privacy: business and technological challenges, Web services and security, Organizational implications of security, Security best practices, Social, political, ethical and psychological dimensions of cybercrime and cyber terrorism, UID Project.

The course will be taught through a series of lectures, readings, project and interactive learning activities.

Evaluation Components:

1. Project (20%)
The project involves in the analysis of the existing information security management scenario of a (your) company based on the learning from this course. The project is expected to identify the risks and limitations of the existing information security management and propose strategies and solutions to meet the current and future challenges for the company. A case of information security breach in the company must be included as part of it. The project requires an interim report (deadline: 25th May 2013 in softcopy) and final report. This is a group project (of 5 members). 6th June 2013 is the deadline for submitting the final report (in hard copy & softcopy - about 20 pages, ppts are not accepted as project reports).

2. Case Presentation (15%)

A standard case study on information security breach is to be presented by every group (same as above) for a duration of 30 minutes. The students can choose a good case study from the literature (but with approval from the instructor on or before 15 May, to avoid conflicts and to ensure quality). Each case discussion is expected to give a true learning experience. The presentation slides need to be submitted (in two days advance). Two presentations each are scheduled on 23 May, 25th May, 30th May, 1st June, and 6th June.

3. Quizzes (15%)

3 online quizzes (15 minutes duration) will be arranged to test student's sharpness of understanding the subject (on 18th May, 30th May, and 8th June).

4. Examination (50%)

A written examination to assess student's competence level on the topics covered.

Note: Choose the topics for Case Presentation and Project by 15th May. Please follow the deadlines.

Text Book:

Godbole N. 2009. Information Systems Security, Wiley India, New Delhi. (GN)

References:

1. Godbole N., Belapure S. 2011. Cyber Security. Wiley- India, New Delhi.
2. Fourouzan N. 2008. Cryptography and Network Security, Tata McGraw-Hill, New Delhi.

Session Plan

Session No.	Topics	Readings	Quiz/Case
1(16th May)	Introduction to Information Security and Privacy, cyber warfare and cyber terrorism, Information security management	GN pages 1-24, 57-85	-
2 (18th May)	Risk analysis, Physical and perimeter security, Biometrics, UID	GN pages 86-165	Quiz
3 (23rd May)	Network security, cryptography	GN pages 167-238	2 Case presentations
4(25th May)	Intrusion detection, firewalls	GN pages 240-276	2 Case presentations
5 (30th May)	VPNs, Wireless and Mobile security	GN pages 26-54, 277-311	2 Case presentations, Quiz
6 (1s June)	Security Models and standards, security metrics	GN pages 397-428, 533-560	2 Case presentations
7 (6th June)	Business Application security, Internet Security Protocols	GN pages 313-358, 680-730	2 Case presentations
8 (8th June)	Privacy: Business challenges and technological impacts, Ethical issues	GN pages 562-678, 897-933	Quiz
9 (13th June)	Security in workplace , Security auditing, Security best practices	GN pages 715-834	-