

# 3000 Information Systems Security

## Introduction

3000 Information Systems Security provides a comprehensive treatment of security management in the context of the information systems environment. With the increasing dependence on technology, security is consistently rated as a major concern amongst customers and corporations alike. The need to provide high levels of security and to create trusted business relationships is a priority for many organisations. This subject covers a broad range of important security topics that include security management, cryptography, access control, network security, application security, operations security, physical security, incident management and business continuity planning (BCP).

### Case studies

A number of real-life case studies are incorporated into the subject to provide opportunities for students to apply theory into practice in an authentic context. Examples of cases include:

Venkatesh, T., G. Kurien and A. Vasudha  
*Indian BPOs: Scandals and the Aftermath*  
 Reference: 906-013-1  
 ICFAI Business School, Bangalore  
 2006

Ho, M. and A. Farhoomand  
*Digital Certificates and Signatures: Microsoft Corporation*  
 Reference: 702-015-1  
 Asia Case Research Centre,  
 The University of Hong Kong  
 2002

Bell, C. and D. Meister  
*A Hacker Attack: An e-Commerce Nightmare*  
 Reference: 9B05E002  
 Richard Ivey School of Business  
 2005

Gordon-Brown, C., K. Slade and N. Duffy  
*Namitech: In the IS Security War Zone*  
 Reference: 904-052-1  
 Wits Business School –  
 University of the Witwatersrand  
 2004

### Who should attend

- Architects and software designers involved in the design of software systems where security is of high concern
- Security managers and IT operations staff with responsibility for information systems security
- Those seeking to develop a broader awareness of information systems security

### Learning objectives

Upon completion of the subject, students should be able to

- conduct a risk assessment
- establish controls for the hiring of employees
- explain the role of cryptography in security management
- define access control policies and formulate penetration and intrusion detection testing plans
- apply security standards such as ITSEC
- advise on appropriate network security procedures
- apply a security plan
- review and advise on security operations
- devise a business continuity plan
- establish policies and procedures for managing security incidents
- devise a facility plan

### Delivery method

The subject is delivered online over a 12-week period, with an assigned Professor acting as mentor. The class will comprise students from different countries and industry backgrounds. Practical assignments and discussions help to stimulate learning and knowledge exchange, while an examination at the end of the subject will help students review and apply the knowledge and skills learnt.

### Prerequisites

Students are recommended to have project experience of systems development work

### Assessment

Assignments (team and individual)	45%
--------------------------------------	-----

Discussion board activities	30%
-----------------------------	-----

Final examination	25%
-------------------	-----

# Syllabus

## Segment 1: Introduction

Students are introduced to the syllabus, the resources and communication tools available within the course.

## Segment 2: Infocomm Security Management

The segment introduces the goals of information and communications security management. Various facets of security management are explained, including security policies and standards, roles and responsibilities, and security awareness education and training. The importance of risk management is described. Students learn about the process of risk management and how to conduct a risk assessment.

## Segment 3: Personnel Security

Hiring trustworthy personnel is an integral part of the security process. The segment looks specifically at employment policies and practices, including the controls needed for hiring, task assignment and termination, within the context of the information systems sector.

## Segment 4: Cryptography

The segment begins with an introduction to basic cryptography concepts, including a comparison between symmetric and asymmetric algorithms. The concept of message integrity is introduced together with the role that security keys play. The area of Public Key Infrastructure (PKI) is explained, and students are encouraged to discuss the role of cryptography on the Internet.

## Segment 5: Access Control

The segment begins with an overview of access control. The various forms of identification and authentication are explained. Access control policies are described, followed by an examination of different access control models and techniques. The role of administration and audit is explained. The dangers of security attacks are highlighted, and detailed guidance is given on how intrusion detection and penetration testing can be used to avert such attacks.

## Segment 6: Trusted Computing Base

The segment examines some of the standards that exist in relation to information systems security. The segment first looks at the concept behind a trust computing base. A number of common security standards used to evaluate computing systems are described, namely the Trusted Computer System Evaluation Criteria (TCSEC) and the Information Technology Security Evaluation Criteria (ITSEC)

## Segment 7: Network Security

This segment opens with an overview of various kinds of networks, including Local Area Networks (LAN), Wide Area Networks (WAN) and the Internet. The various kinds of technologies used to protect networks, such as routers, firewalls and Virtual Private Networks (VPNs) are explained. The segment describes some of the common ways in which networks are attacked, such as denial-of-service attacks.

## Segment 8: Wireless Security

In this segment, the security issues surrounding wireless networks are discussed.

## Segment 9: Application Security

The segment examines security at the application level. Application control security principles are introduced, followed by a discussion of application and database security. This is highlighted by a description of Internet and distributed systems security. Students learn how to devise a security plan.

## Segment 10: Operations Security

The segment describes security at the operations level, beginning with an overview of the operations management area. The concept of system availability is described. A number of key security practices are then examined in detail, namely configuration management, back-ups and audit trails. The importance of systems monitoring is also discussed. To complete the segment, students learn how to identify security vulnerabilities.

## Segment 11: Business Continuity Management

The segment begins by examining the process of contingency planning. Students learn how to conduct a business impact analysis. Further guidance is given on selecting a recovery strategy and developing recovery plans.

## Segment 12: Security Incident Management

The segment begins with a short introduction to legal issues that surround computer security. Evidence management and the computer forensics process are described. Guidance is given on how to set up an incident response team and develop a structured incident response process. The role of ethics in security incidents is also discussed.

## Segment 13: Physical Security

The segment begins with an overview of physical security. Physical access controls, environment controls, technical controls and administrative controls are then described in some detail. To complete the segment, the importance of facility planning is outlined and students learn how to devise a facility plan.

## Required textbook

None

# Global Faculty

## Subject Author

**U21Global subjects are created by acknowledged experts in their field, usually senior academics who have strong understanding of postgraduate requirements. The subject content is further reviewed by academic specialists who appraise the subject from an independent perspective, ensuring a high-quality, professional product.**

3000 Information Systems Security was jointly developed by U21Global and the Institute of Systems Science (ISS), National University of Singapore. ISS specialises in providing professional information technology continuing education to managers and IT practitioners. NUS ranks as one of the top global universities in Asia and Australia.

## Professors

**Students' progress will be guided by dedicated Professor Facilitators based around the world. They provide an international perspective and impart knowledge through a wealth of experience in their field of specialisation. Our Professor Facilitators will help students make sense of the information to enable students to transform the information into knowledge and creative solutions.**



Alok MISHRA

Alok Mishra is Associate Professor of Computer/Software Engineering at Atilim University, Ankara, Turkey. He is also Adjunct Professor at Touro University International in the US. Dr Mishra previously served as a senior faculty member of the Computer Science Department at Jabalpur University in India. He has also taught at the Institut-Latihan-ICL in Kuala Lumpur, Malaysia. Dr Mishra's primary research interests are software engineering, information systems and information systems security, information and knowledge management and object-oriented analysis and design. He has published articles and book reviews related to software engineering and information systems in refereed journals and international conferences. He received his PhD in Computer Science from Jabalpur University.



Michael LAVINE

Michael Lavine is Assistant Professor of Computer and Information Sciences at Towson University, Maryland, US. He is a Visiting Lecturer at the John Cass Business School, City University, London, where he is also Associate Researcher at the Centre for Research in Corporate Governance and Advisory Board Member at the Centre for Internal Auditing. His research interests include information systems, IT auditing, IT security and eCommerce. He has published in several international journals, including the *International Journal of Auditing*, *Review of Accounting Information Systems*, *Review of Business Information Systems*, *Journal of Business Cases*, *The CPA Journal* and *Ohio CPA Journal*, as well as over 20 international conference proceedings.