NATIONAL OPEN UNIVERSITY OF NIGERIA

SCHOOL OF ARTS AND SOCIAL SCIENCES

COURSE CODE: CSS 343

COURSE TITLE:
Information Systems Security Management

Course Guide

CSS 343
Information Systems Security Management

Course Writers/Developers	Dr.A.D Ikuomola (Adekunle Ajasin University)
	Dr. R.A Okunola U.I and Dr. Niyi Adegoke NOUN
Course Editor	Dr. Wole Atere (Osun State University)
Course Coordinators	Dr. Niyi Adegoke NOUN Mr. Igwe, D. O.NOUN Mr. C.A .C. Chukwunka NOUN
Programme Leader	Dr. N.Nwabueze NOUN

CONTENTS **PAGE**

INTRODUCTION

CSS 343 Information Systems Security Management is a 3-credit unit course. It is a compulsory course for both undergraduate and postgraduate students in the field of Criminology and Security Studies of the University. The course is also recommended to any other student(s) particularly those in the school of Arts and Social Sciences, who may have interest in the study and survey of Information Systems Security Management. The course can also be taken as elective or required course by other Students whose main field(s) of discipline is not Criminology and Security Studies. However the course shall consist of 20 units, which include: information gathering, information security in the 21st century: with special emphasis on computer security, introduction to system analysis and design, information system security guide to the use of water quality management principles i and ii, ethics of information communication technology (ICT), identity and information security integration, integrating information assurance into system administration, management information systems usability and associated risk, elevating information security to business security, the information systems and the economics of innocent fraud management, an overview of information security as a risk management function, risk assessment, risk mitigation options, and Mitigating Economic Risk Through Security Technology. The knowledge industry and information communication technology are given special attention with the aim of stimulating effective knowledge of

recent and future methodological and ethical implications of security management, risk assessment options and strategies; the overall safety and security situations and agenda in the world so that students can identify, analyse, and proffer solutions to various aspect of conventional, modern and traditional safety management in the work place and at other civil arena.

The course has no compulsory prerequisite for it to be registered for. The course guide informs us on what this course is all about, what students should appreciate in each unit, what text materials we shall be using and how we can make the best use of these materials. This course guide also emphasises the need for students to take tutor marked assignments seriously. However, necessary information on tutor marked assignments shall be made known to students in a separate file, which will be sent to each of them at the appropriate time. This course is also supported with periodic tutorial classes.

What You Will Learn In This Course

CSS 343: Information Systems Security Management as a course in the field of Criminology and Security Studies at the National Open University of Nigeria focuses on a wide range of issues that bother on ways to effect basic Information Systems Security, knowing quite well that the world today has become smaller in terms of high quality technology similarly accompanied with ever increasing human insecurity with the way and manner crimes are being committed, collapse of business empires and other threats that can jeopardise the safety of any people, industry, community or nation. In this course we will carefully examine, highlight, analyse and assess some issues in Information Systems Security Management. Issues in Information Systems Security Management are usually endless.

Nevertheless, the essence of Information Systems Security Management is at least to provide the students with key issues going on in the world of IT and the knowledge industry, to enhance as well as to make them comfortable in avoiding and if not managing security threats physically or electronically in the cybernetic world. Knowing the impact that active involvement of civilians and non-civilians in security and safety management in an IT world can have, in complementing and increasing the capacity of the security personnel to carry out their duties effectively, the course explores the strategic importance of securing Information and information Systems security through key checklist and models that can contribute to effective safety and security management. For this reason, it is not surprising to see a great number of countries expending huge resources in human, technical and financial terms to fortify their environment against or in readiness for any imagined or perceived threats and abnormal technological or electronic warfare; and owing to the fact that security discourse cannot be complete without looking at issues of science and technology, electronic warfare and global impact of Information systems, trends and patterns now and in the future. This course covers a wide range of issues in the private and public domain regarding Information System

technicalities, problems and solutions to lives and properties, business and military operations.

Course Aims

The overall aim of CSS 343: Information Systems Security Management as a course is to introduce you to information gathering, technology security, access and control, methodology and ethics in computer operations security. It is also aimed at exposing students or readers to knowing most of the existing aspects of Information Security Integration and models, Information Assurance into System Administration, Management Information Systems Useability and Associated Risk vis-à-vis future trends. In furtherance of its overall aim, the material will also help us to explore some other issues like information on modern safety practices, warning signs in mitigating associated security threats.

Undoubtedly, the way the course draws its references from the analysis of various information systems assessments, risk options and models, makes it astounding and thought provoking to providing a pathway for African Students and Scholars in the field of Security Studies to help engender analytical consciousness on the aspects of security in a global world characterised by cyber technology. As you may be aware security issues are always to be considered important and should be given attention. The course is also aimed at understanding:

- Information gathering
- Information security in the 21st century: with special emphasis on computer security
- Introduction to system analysis and design
- Information system security: a guide to the use of water quality management principles
- Ethics of information communication technology (ICT)
- Identity and information security integration
- Integrating information assurance into system administration
- Management information systems useability and associated risk
- Elevating information security to business security
- The information systems and the economics of innocent fraud management
- An overview of information security as a risk management function
- Risk assessment
- Risk mitigation options
- Mitigating economic risk through security technology
- Information age militaries
- Information technology impacts on war fighters
- Information technology and nature of future war
- Difficulties in information security
- The economics of information security investment

Course Objectives

With utmost desire to achieve the aims set out above, the course has some set of objectives as demonstrated in all the units of the course. Each unit has its own objectives. Objectives are always included at the beginning of every unit to assist the student in appreciation of what he or she will come across in the study of each unit to facilitate his or her better understanding of the course CSS 343: Information Systems Security Management. Students are therefore advised to read these objectives before studying the entire unit(s). Thus, it is helpful to do so. You should always look at the unit objectives after completing a unit. In this way, you can be sure that you have done what was required of you by the unit. Stated below are the wider objectives of this course as a whole. By meeting these objectives, you should have achieved the aims of the course as a whole.

At the end of the course, you should be able to:

- Explain information gathering in information system security
- Examine information systems usability and associated risk
- Understand measures in system analysis and design
- Explain the idea behind information security integration into system administration
- Appraise information security as a risk management function
- Understand the relevance of elevating information security to business security
- Discuss ethics of information communication technology (ICT)
- Explain information security in the 21st century
- examine information systems and the economics managing fraud
- Discuss information age militaries
- Examine information technology impacts on war fighters
- Appraise information technology and nature of future insecurity
- Discuss the economics of information security investment
- Highlight factors mitigating economic risk through security technology
- Examine difficulties in information security
- Lastly explain the various ways of assessing information systems risks and mitigation options

Working through this course

In completing this course, students are required to study the whole units, and try to read all (or substantial number of) the recommended textbooks, journals and other reading materials including electronic resources. Each unit contains self assessment exercise(s) and students are required to submit their assignments for the purpose of assessment. At the end of the course, student(s) shall be examined. The time of the final examination and venue shall be communicated to all the registered students in

due course by relevant school authorities-study centre management. Below are the components of the course and what you are required to do:

Course Materials

Major component of the course include:

1. Course Guide
2. Study Units
3. Textbooks
4. Assignments Files
5. Presentations Schedule

It is incumbent upon every student to get his or her own copy of the course material. You are also advised to contact your tutorial facilitator. If you have any difficulty in getting any of the text materials recommended for your further reading.

Study Units

In this course there are twenty units, divided into four modules, (five in each module). Below are the units:

Module 1

Unit 1. Information gathering
Unit 2. Information security in the 21st century: with special emphasis on computer security
Unit3. Introduction to system analysis and design
Unit4. Information system security: a guide to the use of water quality management principles I
Unit5. Information system security: a guide to the use of water quality management principles II

Module 2

Unit 1. Ethics of information communication technology (ICT)
Unit 2. Identity and information security integration
Unit 3. Integrating information assurance into system administration
Unit 4. Management information systems usability and associated risk
Unit 5. Elevating information security to business security

Module 3

Unit 1. The information systems and the economics of innocent fraud management
Unit 2. An overview of information security as a risk management function
Unit 3. Risk assessment
Unit 4. Risk mitigation options
Unit 5. Mitigating economic risk through security technology

Module 4

Unit 1. Information age militaries
Unit 2. Information technology impacts on war fighters
Unit 3. Information technology and nature of future war
Unit 4. Difficulties in information security
Unit 5. The economics of information security investment

Text books, Journals and References

Course Material

The following Text books, and journals are course material recommended to each student taking the course.

Required Readings:

Alberts, David S., John J. Garstka, Richard E. Hayes, and David A. Signori. (2001) *Understanding Information Age Warfare*. Washington, DC: CCRP. August.
Anderson, R.J (2001) *`Security Engineering - A Guide to Building Dependable Distributed Systems'*, Wiley ISBN 0-471-38922-6.

Bartram, J. and Ballance, R. [Eds] (1996) *Water Quality Monitoring. A Practical Guide to the Design and Implementation of Freshwater Quality Studies and Monitoring Programmes.* Published on behalf of UNEP and WHO by Chapman & Hall, London.

Barwise, Jon and John Etchemendy. (2001). "Computers, Visualization, and the Nature of Reasoning." Accessible in PDF format via *http://morpheus.hartford.edu/~anderson/*

Baskerville R & Wood-Harper T (1996) A Critical Perspective on Action Research as a Method for Information Systems Research. Journal of Information Technology 11: 235-246.

Chapman D. and Jackson, J. (1996)Biological monitoring. In: J. Bartram and R. Balance [Eds] *Water Quality Monitoring. A Practical Guide to the Design and Implementation of Freshwater Quality Studies and Monitoring Programmes.* Published on behalf of UNEP and WHO by Chapman & Hall, London, 263-302.

CNN: http://www.cnn.com/2002/US/01/31/rumsfeld.speech/index.html. January 31, 2002. *Network Centric Warfare Department of Defense Report to Congress*. July 2001. pp. 12-14.

Combelles Siegel, Pascale. (1998) *Target Bosnia: Integrating Information Activities in Peace Operations*. Washington, DC: CCRP and National Defense University. January.

Comptroller's Handbook. 1995. Management Information Systems. A Call to Actionfor Corporate Governance. IIA, AICPA, ISACA,NACD, www.theiia.org/eSAC/pdf/BLG0331.pdf; March 2000.

Computer Systems Laboratory Bulletin. *Threats to Computer Systems: An Overview*. March 1994.

Dimensional Advances for Information Architecture," Joanne Twining, *Library Philosophy and*
Practice, Vol. 1 No. 2 (Spring 1999)

Fagin, Robert and Chris Kwak. (2001)*Internet Infrastructure and Services*. Bear Stearns,.

GALBRAITH, John Kenneth (2004): The economics of innocent fraud: Truth for our time, Boston: Houghton Mifflin.

Goetz, E. and Johnson, M.E. (2006) Embedding Information Security Risk Management into the Extended Enterprise: An Executive Workshop, *MacNamee Center for Digital Strategies*, Tuck School of Business at Dartmouth University, USA. Available online at http://mba.tuck.dartmouth.edu/digital/Programs/CorporateEvents/CIO_Ri
skManage/Overview.pdf, accessed on 18 February 2009.

H Varian, Managing Online Security Risks. Economic Science Column, The New York Times, June 1, 2000, http: //www.nytimes.com/library/financial/ columns/060100econ-scene.html

Hayes, Margaret Daly and Gary F. Wheatley, eds.(1996) *Interagency and Political-Military Dimensions of Peace Operations: Haiti—A Case Study*. Washington, DC: National Defense University..

Jim Garamone. (2002). "Flexibility, Adaptability at Heart of Military Transformation." *American Forces Press Service*.

Johnson, D.G. (1994). *Computer Ethics*, second edition; Englewood Cliffs, NJ, Prentice Hall

K.E.Kendell and J.E.Kendell (2002.) Systems Analysis and Design. Pearson Education Asia pp.117-196.

KANT, Immanuel (1795): Perpetual Peace : a philosophical essay, At: http://www.constitution.org/kant/perpeace.txt.

Laudon, K.C., Traver, C.G. and Laudon J.P.(1996). Information Technology and Society, pp.513.

Liu, W., Tanaka, H. and Matsuura, K. (2007) Empirical-Analysis Methodology for Information-Security Investment and Its Application to Reliable Survey of Japanese Firms, Regular Paper, *IPSJ Digital Courier*, 3: 585 – 599.

LOO, Ivo and SOETE, Luc (1999) : 'The Impact of Technology on Economic Growth: Some New Ideas and Empirical Considerations', Research Memoranda 017, Maastricht:

Matsuura, K. (2008) Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model, *The Seventh Workshop on the Economics of Information Security,* 25-28 June 2008, Hanover, USA.

Micki Krause, Harold F. Tipton, (2004). " Handbook of Information Security Management", Vol 1-3 CRC Press LLC.

NIST Special Publication 800-12. *An Introduction to Computer Security: The NIST Handbook*. October 1995.

NIST Special Publication 800-14. *Generally Accepted Principles and Practices for Securing*
Information Technology Systems. September 1996. Co-authored with Barbara Guttman.

NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*. August 2001.

R. M. Fano. (1965).The MAC System: The Computer Utility Approach. *IEEE Spectrum*, 2(1):55–64,

Schrage, Michael. 1990. *Shared Minds: the New Technologies of Collaboration*. New York: Random House.
Shapiro, C. and Varian, H, (1998), *`Information Rules'*, Harvard Business School Press ISBN 0-87584-863-X

Srinidhi, B., Yan, J. and Tayi, G.K. (2008) Firm-level Resource Allocation to Information Security in the Presence of Financial Distress, *Working paper Series 2008-17*, School of Economic Sciences, Washington State University, USA. Available online at www.ses.wsu.edu/PDFFiles/WorkingPapers/Yan/Srinidhi_Yan_GiriJune 2008MISQ.pdf, accessed on 09 February 2009.

Stuart Mc Clure, Joel Scrambray, George Kurtz, 2003 "Hacking Exposed", Tata McGraw-Hill,

Su, X. (2006) An Overview of Economic Approaches to Information Security Management, Technical Report TR-CTIT-06-30, *Centre for Telematics and Information Technology*, University of Twente, Information Systems Group, Enschede, ISSN 1381 – 3625, Netherlands.

Tanaka, H., Matsuura, K. and Sudoh, O. (2005) Vulnerability and Information Security Investment: An Empirical Analysis of e-local Government in Japan, *Journal of Accounting and Public Policy*, Elsevier, 2005(24): 37-59.

V.Rajaraman (2002). Analysis and Design of Information Systems. Prentice Hall of India

Varian, H. (1999). *Intermediate Microeconomics- A Modern Approach'*, Fifth edition, WW Norton and Company, New York,; ISBN 0-393- 97930-0

Varian, H. Managing Online Security Risks", Economic Science Column, The New York Times, June 1, 2000, http://www.nytimes.com/library/financial/ columns/060100econ-scene.html.

Wentz, Larry, ed. (1998) *Lessons from Bosnia: The IFOR Experience*. Washington, DC: CCRP and National Defence University.. pp. 167-187.

Willemson, J. (2006) On the Gordon and Loeb Model for Information Security Investment, presented at *The Fifth Workshop on the Economics of Information Security* (WEIS 2006), University of Cambridge, UK, 26- 28 June 2006. Available online at http://www.ut.ee/~jan/publ/economics.ps, accessed on27 November 2007.

Assignment File

In this file you will find the necessary details of the assignments you must submit to your tutor for assessment. The marks you get from these assignments will form part of your final assessment in this course,

Assessment

There are two aspects to the assessment of the course. First are the tutor-marked assignment; second there is the written examination. In tackling the assignments, you are expected to apply information and knowledge acquired during this course. The assignments must be submitted to your tutor for assessment in accordance with the deadlines stated in the Assignment file. The work you submit to your tutor for assessment will count for 30% of your total course work. At the end of the course, you will need to sit for a final three-hour examination. This will also count for 70% of your total course mark.

Tutor- Marked Assignment

There are twenty tutor-marked assignments in this course. You need to submit four assignments out of which the best three will be used for your assessment. These three assignments shall make 30% of your total course work. Assignment question for the units in this course are contained in the assignment file. You should be able to complete your assignments from the information and materials contained in your set textbooks, reading and study units. However, you are advised to use other references to broaden your view point and provide a deeper understanding of the subject. When you have completed each assignment, send it together with TMA (Tutor-Marked Assignment) file to your tutor. Make sure that each assignment gets to your tutor on or before the deadline. And in case of being unable to complete your work on time, contact your tutor or better still your study centre manager (overseer) before the submission deadline of assignments elapses to discuss the possibility of an extension**.**

Final examination and grading

The final examination of CSS 343 shall be of three hours duration and have a value of 70% of the total course grade. The examination shall consist of questions which reflect the type of self-testing. Practice exercises and tutor-marked problems you have come across. All areas of the course will be assessed. You are advised to revise the entire course after studying the last unit before you sit for the examination. You will find it useful to review your tutor-marked assignments and the comments of your tutor on them before the final examination.

Course Marking Scheme

This table shows how the actual course marking is broken down.

Assessment	Marks
Assignment 1-4	Four assignments are to be submitted, out of which the three best shall be considered at

	10% each, making 30% of the overall scores
Final Examination	70% of overall course marks
Total	100% of course marks.

Table 1: Course Marking Scheme

Course Overview

The table brings together the entire units contained in this course, the number of weeks you should take to complete them, and the assignments that follow them.

Unit	Title	Week's Activity	Assessment (end of unit)
	Course Guide	1	
1.	Information gathering	1	Assignment 1
2.	Information security in the 21st century: with special emphasis on computer security	2	Assignment 2
3.	Introduction to system analysis and design	2	Assignment 3
4.	Information system security: a guide to the use of water quality management principles I	3	Assignment 4
5.	Information system security: a guide to the use of water quality management principles II	4	Assignment 5
6.	Ethics of information communication technology (ICT)	5	Assignment 6
7.	Identity and information security integration	6	Assignment 7
8.	Integrating information assurance into system administration	6	Assignment 8
9.	Management information systems usability and associated risk	7	Assignment 9
10.	Elevating information security to business security	7	Assignment 10
11.	The information systems and the economics of innocent fraud management	8	Assignment 11
12.	An overview of information security as a risk management function	9	Assignment 12
13.	Risk assessment	10	Assignment 13
14.	Risk mitigation options	11	Assignment 14
15.	Mitigating economic risk through security technology	11	Assignment 15
16.	Information age militaries	12	Assignment 16
17.	Information technology impacts on war fighters	13	Assignment 17
18.	Information technology and nature of future war	14	Assignment 18
19.	Difficulties in information security	15	Assignment 19

20.	The economics of information security investment	16	Assignment 20
21.	Revision	17	
22.	Examination	18	

Table 2: Course Overview

Presentation Schedule

The presentation schedule included in your course material gives you the important dates for the completion of tutor-marked assignments and attending tutorials. Remember you are required to submit all your assignments by the due date. You should guard against falling behind in your work.

How To Get The Best From This Course

In distance learning the study units replace the university lecturer. This is one of the great advantages of distance learning; you can read and work through specially designed study materials at your own pace, and at a time and place that suits you best. Think of it as reading the lecture instead of listening to a lecturer. In this same way that a lecturer might set you some reading to do, the study units tell you when to read your set of books or other materials. Just as a lecturer might give you an in-class exercise, your study units provide exercises for you to do at appropriate points. Each of the study units follows a common format. The first item is an introduction to the subject matter of the unit and the course as a whole. Next is a set of learning objectives. These objectives shall let you know what you should be able to do by the time you have completed the unit. You should use these objectives to guide your study. When you have finished the units, you must go back and check whether you have accepted the objectives. If you have a habit of doing this you will significantly improve your chances of passing the course. The main body of the unit guides you through the required reading from other sources.

Reading Section

Remember that your tutor's job is to assist you. Whenever you need help, do not hesitate to call and ask your tutor to provide it.

1. Read this Course Guide thoroughly.

2. Organise a Study Schedule. Refer to the 'Course Overview' for more details. Note the time you are expected to spend on each unit and how the assignments related to the units. Whatever method you choose to use, you should decide on and write in your own dates for working on each unit.

3. Once you have created your own study schedule, do everything you can to stick to it. The major reason why students fail is that they get behind with their course work. If you get into difficulties with your schedule, please let your tutor know before it is too late for help.

4. Turn to Unit 1 and read the introduction and the objectives for the unit.

5. Assemble the study materials. Information about what you need for a unit is given in the 'Overview' at the beginning of each unit. You will almost always need both the study unit you are working on and one of your set books on your desk at the same time.

6. Work through the unit. The content of the unit itself has been arranged to provide a sequence for you to follow. As you work through the units you will be instructed to read sections from your set books or other materials. Use the unit to guide your reading.

7. Review the objectives for each study unit to confirm that you have achieved them. if you feel unsure about any of the objectives, review the study materials or consult your tutor.

8. When you are confident that you have achieved a unit's objectives, you can then start on the next unit. Proceed unit by unit through the course and try to pace your study so that you keep yourself on schedule.

9. When you have submitted an assignment to your tutor for marking, do not wait for its return before starting on the next unit. Keep to your schedule. When the assignment is returned pay particular attention to your tutor's comments, both on the tutor-Marked Assignment form and also on what is written on the assignment. Consult your tutor as soon as possible if you have any questions or problems.

10. After completing the last unit, review the course and prepare yourself for the final examination. Check that you have achieved the unit objectives (listed at the beginning of each unit) and the course objectives (listed in this Course-Guide).

Facilitators/Tutors and Tutorials

There are between eight (8) and twelve (12) hours of tutorials provided in support of this course. The dates, time and venue of these tutorials shall be communicated to you. The name and phone number of your tutor will be made available to you immediately you are allocated a tutorial group. Your tutor will mark and comment on your assignments, keep a close watch on your progress and on any difficulties you might encounter and provide assistance to you during the course. You must mail your tutor marked assignments to your tutor well before the due date (at least two working days are required). They will be marked by your tutor and returned to you as soon as possible. Do not hesitate to contact your tutor by phone, e-mail, or discussion board if you need help. You will definitely benefit a lot by doing that. Contact your tutor if:

- You do not understand any part of the study units or the assigned readings;
- You have difficulty with the self-tests or exercises; and ;

- You have a question or problem with an assignment, with your tutor's comment on an assignment or with the grading of an assignment.

You should make an effort to attend the tutorials. Thus, it is the only opportunity you have to enjoy face contact with your tutor and to ask questions which are answered instantly. You can raise any problem encountered in the course of your study. To gain the maximum benefits from the course tutorials, prepare a question list before attending them. You will learn a lot from participating in discussion actively.

Summary

- CSS: 343 aims to expose you to issues, ideas and methodologies, models in engaging some common technicalities in information Systems Security Management in safeguarding human life in both private and public domains. As you complete this course, you should be able to answer and discuss reasonably the following:

  - ✓ Information security in the 21st century
  - ✓ Information gathering in information system security
  - ✓ Information systems usability and associated risk
  - ✓ Measures in system analysis and design
  - ✓ Information security integration into system administration
  - ✓ Information security as a risk management function
  - ✓ Information security in doing business security
  - ✓ Ethics of information communication technology (ICT)
  - ✓ Examine information systems and the economics of fraud management
  - ✓ Information age militaries
  - ✓ Information technology and nature of future insecurity
  - ✓ Economics of information security investment
  - ✓ Factors mitigating economic risk and security technology
  - ✓ Difficulties and solutions in information systems security management

Finally, you are advised to read the course material appreciably well in order to prepare fully and not to be caught unprepared by the final examination questions. So, we sincerely wish you success in your academic career as you will find this course, CSS 343 very interesting. You should always avoid examination malpractices!

Module 1

Unit 1

INFORMATION GATHERING

Contents

1.0 Introduction

The main purpose of gathering information is to determine the information requirements of an organization. Information requirements are often not stated precisely by management. It is the analyst's responsibility to prepare a precise Systems Requirements

Specifications (SRS), which is easily understood (SRS) by users, as SRS document is a vital document before starting a project

2.0 Objectives

This unit aims at Understanding key points in:

1. Information gathering, strategies, and methods
2. System requirements specification,
3. classification of requirements as strategic, tactical, operational and statutory

3.0 Main body

A strategy should always be available for an analyst to gather information. The strategy consists of identifying information sources, evolving a method of obtaining information from the identified sources and using an information flow model of organization

INFORMATION SOURCES

The main sources of information are users of the system, forms and documents used in the organization, procedure manuals, rule books etc, reports used by the organization and existing computer programs(If Any).

INFORMATION GATHERING METHODS: SEARCHING FOR INFORMATION

Information can be gathered by interviewing top-level management, middle level management and operational staff. Besides Interviews group discussions also help the analyst to gather information. It is not possible to obtain all information in a single interview, more than one interview is thus required.

PLANNING AN INTERVIEW

Before starting the interview the analyst must make a list of people to be interviewed and in what order, plan and note down a list of questions to be asked, plan several interviews with same person-mainly to clarify doubts and interview groups as appropriate.

INTERVIEWING TECHNIQUE

There are some guidelines to ensure a successful interview: Make a prior appointment with the person to be interviewed and meet him at the allotted time. Read background material and go prepared with the checklist. State purpose of interview. Be punctual and pay attention to what user says. Do not use computer jargon. Obtain both quantitative and qualitative Information. Discriminate between essential and desirable requirements. State what you understand and get it confirmed. Do not prolong interview and summarize the information gathered by you during the interview and verify this with the user

USE OF QUESTIONNAIRES

Questionnaires are useful for collecting statistical data. Sometimes the questionnaires are not promptly replied and several follow-ups/personal interviews may be required to get

questionnaires back from respondents But if the questionnaires are short the probability of getting the reply is high When data has to be collected from large number of people questionnaires are useful.

OTHER METHODS OF INFORMATION GATHERING

Other methods of information search are:

1. Systems used in other similar organization
2. Observe workflow in workplace
3. Repository of systems developed for similar organizations available.

SYSTEM REQUIREMENTS SPECIFICATION (SRS)

SRS is obtained after extensive discussions with the user. System requirements specification specifies what Information requirements will be provided. It does not specify how the system will be designed. Developing SRS is most important and difficult task of a Systems analyst

How SRS is developed

An analyst examines the current system, finds out the shortcomings of the system as seen by the user. He then develops an SRS which is understandable by the user and which can be used for detailed design of the system.

Ideal characteristics of SRS

- Complete and Unambiguous.
- Specifies operational, tactical, and strategic information requirements
- Eliminates possible later disputes between users and Analyst
- Uses Graphical aids understood by users who are not computer literate and will also be useful in design.
- Jargon Free.

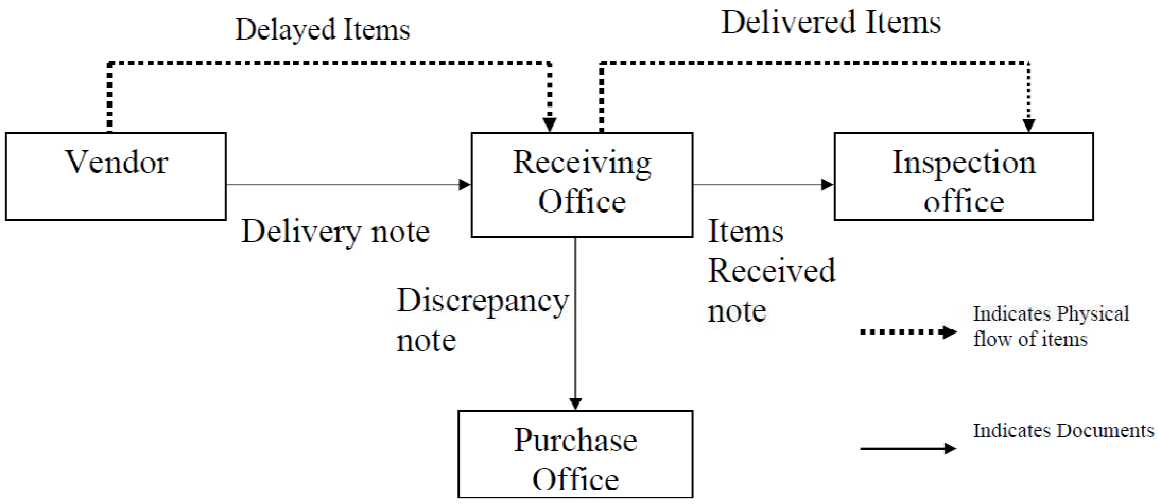
DEVELOPING A DOCUMENT FLOW DIAGRAM

EXAMPLE WORD STATEMENT

“Our company receives many items from several vendors each accompanied by a delivery note. A receiving office receives the item and checks the delivery note with corresponding order. Any discrepancy is reported to purchase office. The items received along with items received note (with details of items) is sent to the inspection office.”

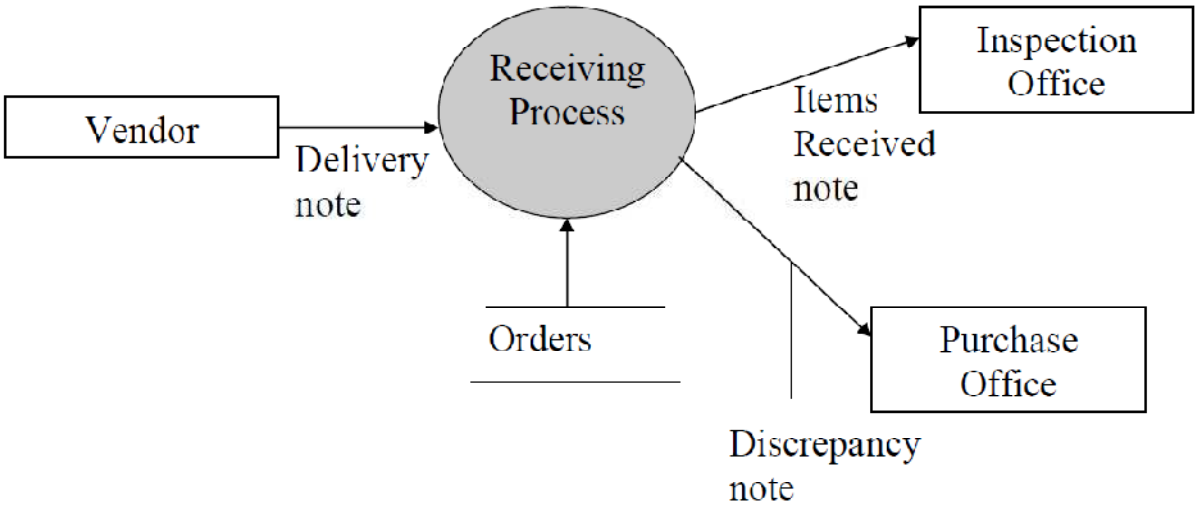
ENTITIES IDENTIFIED-Vendors, Receiving office, Inspection office
DOCUMENTS IDENTIFIED-Delivery note, discrepancy note, Items

Received note.
Using these a document flow diagram is drawn



The diagram is interpreted as follows:
1) Vendors deliver items to receiving office accompanied by a delivery note
2) Receiving Office sends items to inspection office along with an items received note
3) Receiving office sends discrepancy note to Purchase office
ENTITIES: Vendor, Receiving office, Inspection office and purchase office
DOCUMENTS: Delivery note, Items received note and discrepancy note

DATA FLOW DIAGRAM (DFD)
DFD has entities and data flows, DFD specifies processing performed by some of the entities. It specifies which entities generate documents and also indicate their flow. Data stores which are referred while processing data and in which processed data may be written or stored are also represented in the Diagram



- Entities are, originators of data and “consumers” of data
- Vendor, Inspection office and purchase office are entities in the above diagram
- Data flows are delivery note; items received note and discrepancy note
- A circle is used to depict a process
- A pair of parallel lines depicts a store

Data elements in the data flow:

Delivery note:
Order number, Vendor code, Vendor name and address, Item name, Item code, Delivery date, Quantity supplied, units.

Items Received note:
Order number, Item name, Item code, Delivery date, quantity, supplied, units.

Discrepancy note:
Order number, Vendor code, Vendor name and address, Item name, Item code, Order date, Delivery date, quantity supplied, units, excess/deficiency, Number of days late/early.

Receiving office order file
Order number, Order date, Item name, Item code, Vendor code, Vendor Name and address, Quantity ordered, delivery period.

PROCESSING RULE
The statements given below are shown to the user for his approval.

English statement

1. Compare order number in delivery note with that in order file. If no match return item to vendor.
2. If order number matches then compare item codes, if no match return item to the vendor.
3. If order number matches compare quantity delivered with quantity ordered. If excess or deficient send discrepancy note to purchase office.
4. If order number matches compare date of delivery with expected date. If late or early send discrepancy note to purchase office.
5. In case3 and case4 send items received note to inspection office

MODULARIZING REQUIREMENTS SPECIFICATIONS

SRS Document now consists of Document flow diagrams(as many as needed), Data Flow Diagrams, Data elements of each data flow and Data store, processing rules carried out in each circle of DFD, a descriptive statement of operational, tactical, strategic information will be provided, a data dictionary which consolidates all data elements in the document and data store.

Assessment and Exercise

1. List and explain some information sources.
2. Information gathering can be difficult. Explain

4.0 Conclusion

The Information system designed for an organization must meet the requirements of the end users of the organization. To obtain what an end user expects from the Information System the designer must gain complete knowledge of the organization's working. It is important for student to know the information gathering techniques so that no information is overlooked and the nature and functions of an organization are clearly understood.

5.0 Summary

This units explains some specific strategies of gathering information (information sources) for computerization. Various sources of information such as the interviews, and questionnaire as well as how best to plan and make use of them by individuals in any organization.

6.0 Tutor Marked Assignment

Hypothetically choose a company name and develop a document and data flow diagram.

7.0 References/ Further Reading

V.Rajaraman 2002. Analysis and Design of Information Systems. Prentice Hall of India

K.E.Kendell and J.E.Kendell 2002. Systems Analysis and Design. Pearson Education Asia pp.117-196.

Barwise, Jon and John Etchemendy. (2001). "Computers, Visualization, and the Nature of Reasoning." Accessible in PDF format via *http://morpheus.hartford.edu/~anderson/*

Dimensional Advances for Information Architecture," Joanne Twining, *Library Philosophy and*
Practice, Vol. 1 No. 2 (Spring 1999)

Schrage, Michael. 1990. *Shared Minds: the New Technologies of Collaboration*. New York: Random House.

Unit 2

Information Security In The 21st Century: With Special Emphasis on Computer Security

Contents

1.0 Introduction

Information security deals with several different 'trust' aspects of information. Another common term is information assurance. Information security is not confined to computer systems, nor to information in an electronic or machine-readable form. It applies to all aspects of safeguarding or protecting information or data, in whatever form. Information security chain is needed when information is threatened, lost or misused.

2.0 Objectives

The unit is aimed at presenting the need of information security in 21st century. Students are expected to know:

1. What information security is?
2. Why it is needed in an organization of the 21st century.
3. The confidentiality, integrity and availability (CIA) Relationship of information security.

3.0 Main body

Information security is a protection of the interests of those who rely on information, the information systems and communications that deliver the information from harm resulting from failures of availability, confidentiality, and integrity.
The organization's information security policy aims to ensure that:

- Its information systems are properly assessed for security
- Confidentiality, integrity and availability (CIA) are maintained. These three concepts are at the core of almost every security program—if not by name, at least in practice. They are most commonly described as a triangular view of security, with each side directly related to the other two. As shown in Figure1. Confidentiality – information access is confined to those with specified, explicit authority to view the information.

Integrity – safeguarding the accuracy and completeness of information. Availability – ensuring that authorized users have access to information when needed.

- Staff are aware of their responsibilities, roles and accountability
- Procedures to detect and resolve security breaches are in place
- Information security issues are dealt with consistently throughout the organization

Figure 1:

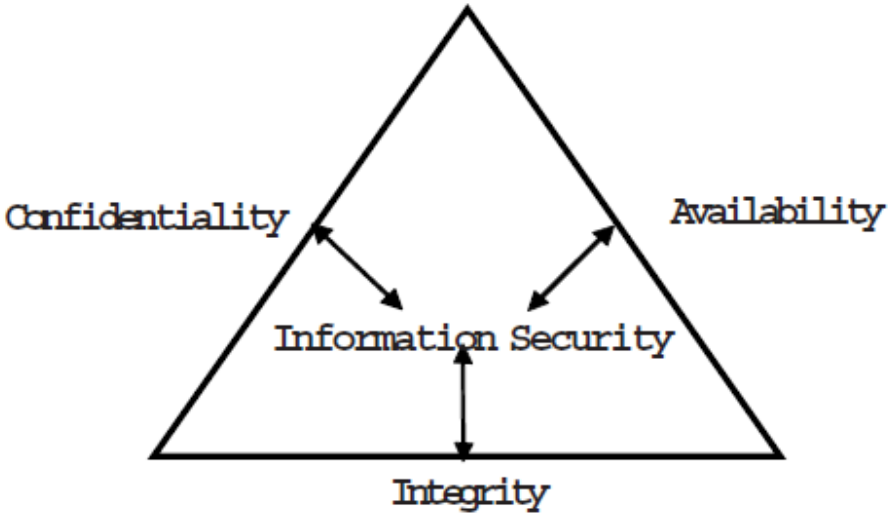


Figure 1: The CIA Relationship

What Is Information Security?

We are a part of an information Society. Huge amount of Information can be speedily processed and saved on easily accessible media. Information plays a really important part in decision making in an organization. For an organization a wrong decision can lead to drastic result. This is one of the reasons why information security is steadily acquiring a more central role in business. In the world of today information is becoming increasingly important. Generally speaking the standard of information security has not kept pace with this development. For example, information that before was saved on a large amount of paper and physically difficult to steal can today be saved on a disk that can easily be removed. Information security is an attempt to protect information by making it accessible only to the intended individuals, groups or organizations. The reason may be financial, political, tactical or purely logistical. Every organization depending upon its resources, and the type of data it handles, has allowed a separate budget and manpower for developing information security arrangements. According to Dr. Thomas V. Finne information security chain has twelve modules and eighty sub-modules as below:

1. **Computer Security** : This module includes seventeen submodules - Backup, Computer Viruses, Passwords, Data Encryption, Biometric Methods, Off-site Storage, System Backup, Cold and Hot Sites, Card Access, Disk-Free Station, Computer Locks, Printer and Fax Security, Diskette Security, Rescue Diskette, Distributed Systems, Outsourcing, Time Sharing and Remote Office, Log Functions, Locked Hardware.

2. **Operation Security**: Software Security, Illegal use of Software, Spread sheeting and DSSs, Data Input Security, Data File Destruction, Data Compression, Utility Programs, System Administration, Data Leakage, Super zapping, Entrapment, Database.

3. **Protection against Burglary**: Security Guards, Alarms, Access Control, Safes.

4. **Protection against Fire**: Alarms, Sprinklers, Fireproof Safes and Cupboards.

5. **Protection against Water Damage**: Building Materials and Construction, Water Sensors, Flooding.

6. **Electricity Distribution**: The Electricity Supply, Allergy to Electricity, Magnetic Fields, Electromagnetic Fields.

7. **External and Internal Threats**: Sabotage, Espionage, Abuse, Public Information.

8. **Communication**: Telephone Lines, Cable Security, External Contact, Dial-up, Firewalls, Mobile Computing.

9. **Contingency Planning**: Emergency, Recovery.

10. **Personnel Security**: Recruiting, Control of Personnel, Access to Information, Human Mistake, Contract Employees and Visitors, Unauthorized Work, Staff Shortage, Theft by Staff, Impersonation, Piggybacking, Officer Appointed to be Responsible for information security (ISEC), ISEC Education, Incident Reporting.

11. **Attitudes toward ISEC Issues**: Written Security Policy, Information Security Culture.

12. **Various Security Questions**: Atmospheric Humidity, Document Security, Temperature, Dust, Smoke, and Particles, Optical Spying, the Environment, Tailgating, Scavenging, Shoulder Surfing, Building, Mail Security.

Computer Security

Computer security measures, procedures, and controls which provide an acceptable degree of safety of information resources from accidental or intentional disclosure, modification, or destruction. Sub modules of computer security are as below.

A. Backup

Backup means having multiple copies of the same data so that the duplicate ones can be used in case the original one gets corrupted or erased accidentally. Though having backups may seem as a waste of time but they often come in handy when one actually needs them. Backups must also be tested so as to avoid failure owing to human or machine malfunctioning. Of the different media that can be used for doing backups it is important to have effective, reliable and user friendly backup software. Instead of having a backup of all the files, it is advised to have it for just the most important ones.

B. Computer Viruses

Viruses are defined as 'A section of code introduced into a program for malicious purposes, e.g. at some stage the inserted code will trigger a process which will, for example, eliminate files. The virus is present in a program, and when the program is run the virus writes itself into other programs in main memory or backing store. The effects of virus can thus be extended to many users'. There are many kinds of computer viruses like Worms, Bombs, Trojan horses and Computer viruses. A way to avoid computer viruses is always to test the software before installing it and to avoid pirated software. Viruses can be spread through emails also. Some of the most well known viruses are Bugbear, Klez, Lovebug, Melissa, Bubbleboy, Code Red, Nimda. There are six recognized categories of virus as below:

i. **Boot Sector Virus:** Replaces or implants itself in the boot sector—an area of the hard drive (or any other disk) accessed when you first turn on your computer. This kind of virus can prevent you from being able to boot your hard disk. Eg. Disk Killer, Michelangelo, stoned.

ii. **File Virus:** Infects applications. These executables then spread the virus by infecting associated documents and other applications whenever they're opened or run. Eg. Jerusalem and Cascade.

iii. **Macro Virus:** Written using a simplified macro programming language, these viruses affect Microsoft Office applications, such as Word and Excel, and account for about 75 percent of viruses found in the wild. A document infected with a macro virus generally modifies a pre-existing, commonly used command (such as Save) to trigger its payload upon execution of that command. Eg. W97M.Melissa, WM.NiceDay, W97M.Groov.

iv. **Multipartite Virus:** Infects both files and the boot sector—a double whammy that can re- infect your system dozens of times before it's caught. Eg. One_Half, Emperor, Anthrax, Tequilla.

v. **Polymorphic Virus:** Changes code whenever it passes to another machine; in theory these viruses should be more difficult for antivirus scanners to detect, but in practice they're usually not that well written.

vi. **Stealth Virus:** Hides its presence by making an infected file, not appear infected, but doesn't usually stand up to antivirus software.

- **Worm**

A worm is a program that is designed to replicate and spread throughout a computer system. It will usually hide within files (for example, Word documents), and distribute those files through any available network connections. Worms are often used to drain computer resources such as memory and network access, simply by replicating on a large scale. Eg. W32.Mydoom.Ax@mm

- **Trojan Horse**

A Trojan horse is a malicious program, usually disguised as something useful or desirable. When activated, they can cause loss, damage or even theft of data. The critical difference between a Trojan horse and a virus is that a Trojan horse cannot replicate itself. The only way that a Trojan horse can spread is if someone helps it. Trojan.Vundo is a Trojan. For example, saving the program from an e-mail attachment, or downloading it from the Internet. Some common features of Trojan horse programs include:

a. Rounding (carving off small parts of payments from a large number of accounts or transactions),
b. Causing payment triggers (causing illicit payments to be activated),
c. Making configuration changes,
d. Distributing security information, providing unauthorized access paths (known as backdoors and trapdoors).

- **Precautions**

Protection against Computer Viruses, Worms and Trojans are :

I. Run antivirus software recommended from the information security division of organization and make sure that version is current and the latest.
II. Don't open macros attach files from unknown email. Delete these attachments immediately.
III. Delete spam, chain, and other junk email without forwarding.
IV. Don't download files or email attachments from unknown or unauthorized sources.
V. Scan a floppy diskette from an unknown source for viruses before using it.

New viruses are discovered almost every day. Up-date of anti-virus software should be done only through designated sources, and do not trust any other sources for virus

protection patches. Common among these viruses are Trojan.Advatrix, Trojan.Sushpy, Trojan.Nssearch, Bloodhound.Exploit.163, and W32.Usbwatch .

C. Passwords

These play significant role in computer security. Passwords should be complicated and should contain both numbers and letters. The passwords should not have user's name, license plates etc. but some imagination should be used. Every computer user in an organization has to observe good password security. Their password security can be checked, however because once a user selects a password, the system administrator can use a password checker to automatically check if the password is suitable. In a company where there are several servers and networks in use. The user has to remember many passwords. In this case the user tends to use similar passwords for different systems, which in turn increases the security risk. Thus to avoid this access control packages that includes passwords, logs, encryption and so forth must be used. By using such packages it can be possible to avoid using many password systems. Vendor supplied passwords should be changed immediately.

D. Data Encryption

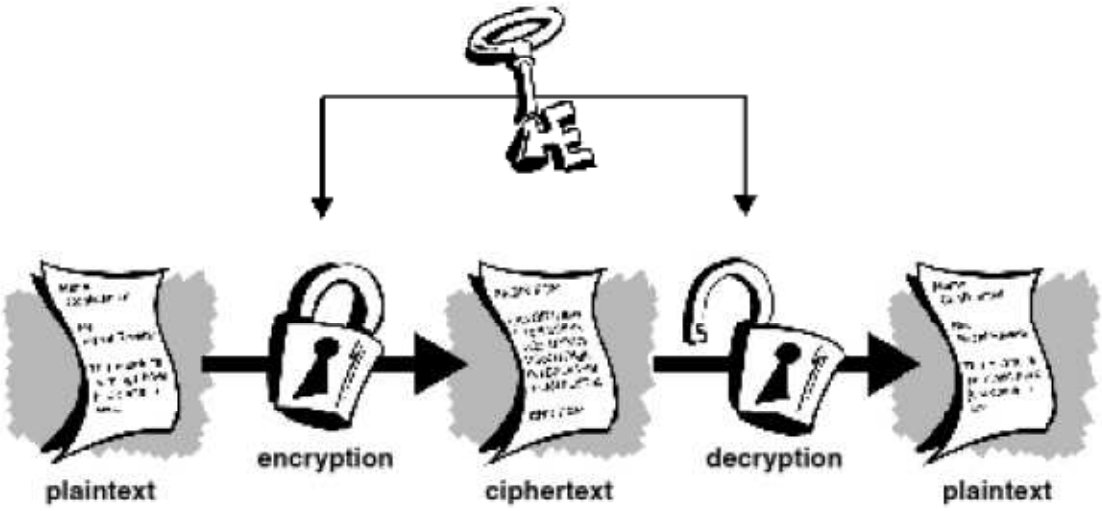
Data encryption is a means of securing data by changing the meaningful text into some code which looks like null and void to others. It's a reasonably easy way to protect information. The user has to remember the key and the software and hardware is secure and user friendly. According to Hoffman there are 900 cryptography hardware and software products on the market. The System administrator normally has access to all files in an information system, therefore the administrator can be a great information security risk, and the risk can be minimized, however, if the classified files are encrypted. The administrators still do his work.

i. How does Encryption Work?

Encryption involves taking an original message or plaintext and converting it into cipher text (unreadable format) using an encryption algorithm and an encryption key. Only those who posses a secret key can decipher the message into plain text. Historically, encryption acted on letters of the alphabet. The Caesar Cipher, one of the oldest techniques, gives a very simple example:

a. Take the plaintext is Parliament is in session;
b. Encrypt according to the encryption algorithm 'replace each letter with that X places to the right of it in the alphabet', where X, the encryption key, is 3;
c. The cipher text is sduoldphqw lv lq vhvvlrq and can be converted back to plaintext with a decryption algorithm and decryption key, in this case 'replace each letter with that three places to the left of it in the alphabet'.

Computers store electronic data in binary form, as sequences of ‘bits’ (1s and 0s). Modern algorithms are mathematical functions that act on these data with keys that are themselves sequences of 1s and 0s. Keys are generally stored in computer files that are themselves encrypted and can be accessed only with a pass phrase (similar to a password but longer). We can see its working Figure 2. Encrypted messages can sometimes be broken by cryptanalysis (coding breaking) but modern cryptography techniques are virtually unbreakable, eg. Cryptography is to protect- email messages, credit card. Most popular systems used on the internet are Pretty Good Privacy because it is effective and free.



E. Biometric Methods

Biometric methods include those of voice, face, hand geometry, fingerprints, eye, signature and typing rhythms as shown in Figure 3. When combined with good password security, can give high information security but it needs high cost biometric instruments.

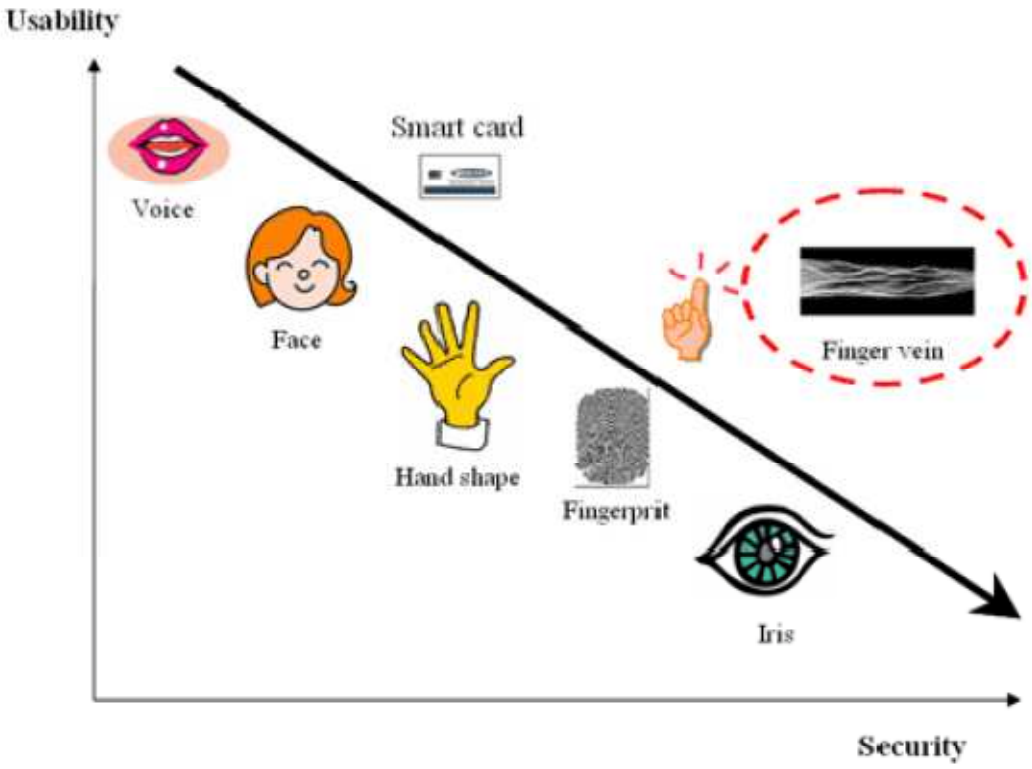


Figure 3: Examples of Biometric Methods

F. Off-Site Storage

Off-site storage means storing the backup files in a secure place. They should preferably be encrypted. So many commercial organizations are available in the market, specializing in storing 'organization backup'. So there is no need to build one's own storage facilities. The organization storing the backups has to be extremely reliable.

G. System Backup

Most organizations think that system backups (backup of networks) are unnecessary because the software is easily available from the distributors. On the contrary it is a nice practice to have spare systems which are tested regularly.

H. Cold and Hot Sites

Cold sites are empty computer rooms with everything besides computers and communications systems installed. For example, in case of emergency (fire, earthquakes etc,) computer centre destroyed, it can be useful to have a cold site. Hot sites on the other hand are fully equipped "spare" computer centers. These are recommended for organizations with an extremely heavy reliance on computers. Spare computer centre can be approximately 50 percent of the capacity of the original one. Both hot and cold sites can be shared by many organizations.

I. Card Access

Using plastic cards for accessing PCs can improve information security in an organization. It is usually combined with the use of a personal code. Cards can be provided with the photograph of the user too. A log in a microcomputer can register when a card is used. To avoid unauthorized use of a card, lost cards have to be blocked immediately.

J. Disk-free Stations

Use of disk-free stations and passwords to access the server can minimize information security problems in an organization where there are hundreds of PCs connected in a network. By this only a few key persons will have authorization to copy information on to diskettes.

K. Computer Locks

Servers should be provided with a computer lock in its disk station. The key to the computer should be kept safe and must not be lost. The PCs are provided with an inbuilt lock that can be used to shut them off.

L. Printer and Fax Security

Printers should not be provided with terminals if it is possible to take printouts of classified material. Printers should be kept in locks. In an organization it is common that many people share a printer. This means that the material printed out can be seen by many people and if the printer is not kept behind locked doors. There can be considerable damage. Another considerable problem with faxes is that the sender can easily dial the wrong number by mistake. Managers should have their own fax machine. This naturally implies that the managers are reliable enough and they do not use the fax for sending out documents to a competitor.

M. Diskette Security

A diskette containing important information should not be sent by mail. Such a procedure should be avoided since the diskette can be stolen, copied, or damaged during transportation. Electronic data interchange should be used. Diskettes are stored properly in a safe place and in an organized manner.

N. Rescue Diskette

Rescue diskette should include the most important utilities, in the case of a PC, especially the .com, .dat, .exe, .ini and .sys files. The rescue disk can be very useful, when a user is attacked by computer viruses. The rescue diskette has to be properly stored.

O. Distributed Systems, Outsourcing, Time Sharing and Remote Office

Distributed systems, outsourcing, time sharing and remote office are fairly new processes in IT which bring new information security concepts. **Distributed system** means moving from traditional large computers to open client / server systems. In distributed environment every employee's responsibility for information security increases. **Time**

sharing means that organizations share computing services and in that way decrease costs. Risk increase in this. The resources saved by using shared premises and **outsourcing** can easily be lost in an information security break. Those involved have to be extremely reliable. **Remote office** means carrying out the work at home or at another location by means of modern telecommunication. Data transmission should be encrypted. Information security must not hinder an organization from carrying out a remote office operation, but the questions for information security have to be observed.

P. Log Functions

A log function registers when a PC was used. By using a log it is possible to determine, afterwards, if files have changed in order to commit a fraud.

Q. Locked Hardware

Hardware should be locked, for example, office furniture etc. This makes it more difficult to steal the hardware. Thieves are interested in only Computers and especially hard disks.

Self Assessment Exercise

1. What is Data Encryption?
2. How does it work?

4.0 Conclusion

Information security is the ongoing process of exercising due care and due diligence to protect information, and information systems, from unauthorized access, use, disclosure, destruction, modification, or disruption. The academic disciplines of information security and information assurance emerged along with numerous professional organizations during the later years of the 20th century and early years of the 21st century. The profession of information security chain has seen an increased demand for security professionals who are experienced in network security auditing, penetration testing, and digital forensics investigation. So to secure an organization there is a need of information security in the 21st century organization**.**

5.0 Summary

This unit discusses what information security is. Why it is needed in an organization of the 21st century. The CIA Relationship of information security is discussed with diagram. The information security chain has twelve modules and eighty sub modules. Lastly, the future and conclusion of information security are highlighted. The unit is of particular value for newcomers in this area.

6.0 Tutor Marked Assignment

a. What is information security?
b. Succinctly define and list some Computer Viruses known to you, and
c. How can they be guided against?

7.0 References/ Further Reading

Caelli, W. D. (1989). Longley and M. Shain, Information Security for Mangers, Stockton, Uk, 1989. http://www.symantec.com/business/security_response/threatexplorer/threats.jsp accessed on October 26, 2007.

Hoffman, L. (1995). Encryption Policy for the Global Information Infrastructure, in Information Security: the next Decade, J. Eloff and S. Von Solms, ed. proceedings of the IFIPTC11 Eleventh International Conference on Information Security, South Africa, May 9-12, 1995, pp 50-63.

Managing security of information of information technology committee, website at www.ifac.org/new. (IFAC 1998. Exclusive Summary).

Maynard, J. (1994), Computer Audit Update, UK, Dec. pp 15-18 http://www.iitk.ac.in/cc/services.htm#login accessed October 27, 2007.

Smith, M. (1993). Commonsense Computer Security; your practical guide to information security. McGraw Hill, London.

Thomas V. Finne (2001). Encyclopedia of Library and Information Science By Allen Kent Marcel Dekker, New york V.65 p.p 139-166.

Wood, C.C. (1991). Effective Information Security Management, Elsevier Advanced Technology, Oxford, UK,

Unit 3

Introduction to System Analysis and Design

Contents

1.0 Introduction

Systems are created to solve problems. One can think of the systems approach as an organized way of dealing with a problem. In this dynamic world, the subject System Analysis and Design (SAD), mainly deals with the software development activities.

2.0 Objectives

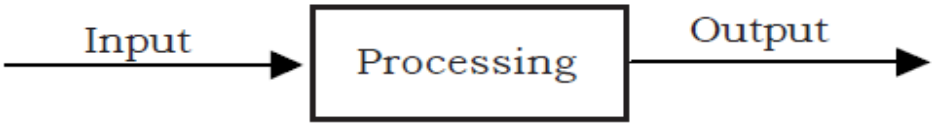
After going through this lesson, you should be able to:

- define a system
- explain the different phases of system development life cycle
- enumerate the components of system analysis
- explain the components of system designing

3.0 Main body

DEFINING A SYSTEM
A collection of components that work together to realize some objectives forms a system. Basically there are three major components in every system, namely input, processing and output.

Fig. 1.: Basic System Components



In a system the different components are connected with each other and they are interdependent. For example, human body represents a complete natural system. We are also bound by many national systems such as political system, economic system, educational system and so forth. The objective of the system demands that some output is produced as a result of processing the suitable inputs. A well-designed system also includes an additional element referred to as 'control' that provides a feedback to achieve desired objectives of the system.

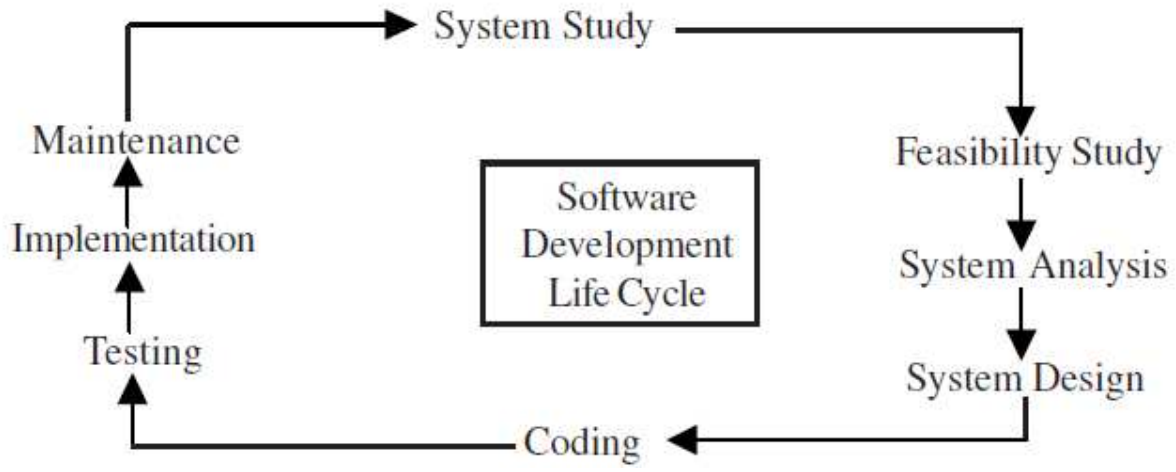
SYSTEM LIFE CYCLE

System life cycle is an organizational process of developing and maintaining systems. It helps in establishing a system project plan, because it gives overall list of processes and sub-processes required for developing a system. System development life cycle means combination of various activities. In other words we can say that various activities put together are referred to as system development life cycle. In the System Analysis and Design terminology, the system development life cycle also means software development life cycle.

Following are the different phases of system development life cycle:

- Preliminary study
- Feasibility study
- Detailed system study
- System analysis
- System design
- Coding
- Testing
- Implementation
- Maintenance

The different phases of system development life cycle is shown in Fig. 2 below.



Phases of System Development Life Cycle

PHASES OF SYSTEM DEVELOPMENT LIFE CYCLE

Let us now describe the different phases and related activities of system development life cycle.

(a) Preliminary System Study

Preliminary system study is the first stage of system development life cycle. This is a brief investigation of the system under consideration and it gives a clear picture of what actually the physical system is? In practice, the initial system study involves the preparation of a 'System Proposal' which lists the Problem Definition, Objectives of the Study, Terms of reference for Study, Constraints, Expected benefits of the new system, etc. in the light of the user requirements. The system proposal is prepared by the System Analyst (who studies the system) and places it before the user management. The management may accept the proposal and the cycle proceeds to the next stage. The management may also reject the proposal or request some modifications in the proposal. In summary, we would say that system study phase passes through the following steps:

i. problem identification and project initiation
ii. background analysis
iii. inference or findings (system proposal)

(b) Feasibility Study

In case the system proposal is acceptable to the management, the next phase is to examine the feasibility of the system. The feasibility study is basically the test of the proposed system in the light of its workability, meeting user's requirements, effective use of resources and of course, the cost effectiveness. These are categorized as technical, operational, economic and schedule feasibility. The main goal of feasibility study is not to solve the problem but to achieve the scope. In the process of feasibility study, the cost and benefits are estimated with greater accuracy to find the Return on Investment (ROI). This also defines the resources needed to complete the detailed investigation. The result is a feasibility report submitted to the management. This may be accepted or accepted with modifications or rejected. The system cycle proceeds only if the management accepts it.

(c) Detailed System Study

The detailed investigation of the system is carried out in accordance with the objectives of the proposed system. This involves detailed study of various operations performed by a system and their relationships within and outside the system. During this process, data are collected on the available files, while decision points and transactions handled by the present system. Interviews, on-site observation and questionnaire are the tools used for detailed system study. Using the following steps it becomes easy to draw the exact boundary of the new system under consideration:

- Keeping in view the problems and new requirements
- Workout the pros and cons including new areas of the system

All the data and the findings must be documented in the form of detailed data flow diagrams (DFDs), data dictionary, logical data structures and miniature specification. The main points to be discussed in this stage are:

- Specification of what the new system is to accomplish based on the user requirements.
- Functional hierarchy showing the functions to be performed by the new system and their relationship with each other.
- Functional network, which are similar to function hierarchy but
- they highlight the functions which are common to more than one procedure.
- List of attributes of the entities – these are the data items which need to be held about each entity (record)

(d) System Analysis

Systems analysis is a process of collecting factual data, understanding the processes involved, identifying problems and recommending feasible suggestions for improving the system functioning. This involves studying the business processes, gathering operational data, understanding the information flow, finding out bottlenecks and evolving solutions for overcoming the weaknesses of the system so as to achieve the organizational goals. System Analysis also includes subdividing of complex process involving the entire system, identification of data store and manual processes. The major objectives of systems analysis are to find answers for each business process: What is being done, How is it being done, Who is doing it, When is he doing it, Why is it being done and How can it be improved? It is more of a thinking process and involves the creative skills of the System Analyst. It attempts to give birth to a new efficient system that satisfies the current needs of the user and has scope for future growth within the organizational constraints. The result of this process is a logical system design. Systems analysis is an iterative process that continues until a preferred and acceptable solution emerges.

(e) System Design

Based on the user requirements and the detailed analysis of the existing system, the new system must be designed. This is the phase of system designing. It is the most crucial phase in the development of a system. The logical system design arrived at as a result of systems analysis is converted into physical system design. Normally, the design proceeds in two stages:

i. Preliminary or General Design
ii. Structured or Detailed Design

Preliminary or General Design: In the preliminary or general design, the features of the new system are specified. The costs of implementing these features and the benefits to be derived are estimated. If the project is still considered to be feasible, we move to the detailed design stage.

Structured or Detailed Design: In the detailed design stage, computer oriented work begins in earnest. At this stage, the design of the system becomes more structured. Structure design is a blue print of a computer system solution to a given problem having the same components and inter-relationships among the same components as the original problem. Input, output, databases, forms, codification schemes and processing specifications are drawn up in detail. In the design stage, the programming language and the hardware and software platform in which the new system will run are also decided. There are several tools and techniques used for describing the system design. These tools and techniques are:

1. Flowchart
2. Data flow diagram (DFD)
3. Data dictionary
4. Structured English
5. Decision table
6. Decision tree

The system design involves:

I. Defining precisely the required system output
II. Determining the data requirement for producing the output
III. Determining the medium and format of files and databases
IV. Devising processing methods and use of software to produce output
V. Determine the methods of data capture and data input
VI. Designing Input forms
VII. Designing Codification Schemes
VIII. Detailed manual procedures
IX. Documenting the Design

(f) Coding

The system design needs to be implemented to make it a workable system. This demands the coding of design into computer understandable language, i.e., programming language. This is also called the programming phase in which the programmer converts the program specifications into computer instructions, which we refer to as programs. It is an important stage where the defined procedures are transformed into control specifications by the help of a computer language. The programs coordinate the data movements and control the entire process in a system. It is generally felt that the programs must be modular in nature. This helps in fast development, maintenance and future changes, if required.

(g) Testing

Before actually implementing the new system, a test run of the system is done for removing the bugs, if any. It is an important phase of a successful system. After codifying

the whole programs of the system, a test plan should be developed and run on a given set of test data. The output of the test run should match the expected results. Sometimes, system testing is considered a part of implementation process.
Using test data, the following test run are carried out:

- Programme test
- System test

Program test: When the programs have been coded, compiled and brought to working conditions, they must be individually tested with the prepared test data. Any undesirable happening must be noted and debugged (error corrections)

System Test: After carrying out the program test for each of the programs of the system and errors removed, then system test is done. At this stage the test is done on actual data. The complete system is executed on the actual data. At each stage of the execution, the results or output of the system is analyzed. During the result analysis, it may be found that the outputs are not matching the expected output of the system. In such case, the errors in the particular programs are identified and are fixed and further tested for the expected output. When it is ensured that the system is running error-free, the users are called with their own actual data so that the system could be shown running as per their requirements.

(h) Implementation
After having the user acceptance of the new system developed, the implementation phase begins. Implementation is the stage of a project during which theory is turned into practice. The major steps involved in this phase are:

- Acquisition and Installation of Hardware and Software
- Conversion
- User Training
- Documentation

The hardware and the relevant software required for running the system must be made fully operational before implementation. The conversion is also one of the most critical and expensive activities in the system development life cycle. The data from the old system needs to be converted to operate in the new format of the new system. The database needs to be setup with security and recovery procedures fully defined. During this phase, all the programs of the system are loaded onto the user's computer. After loading the system, training of the user starts. Main topics of such type of training are:

1. How to execute the package
2. How to enter the data
3. How to process the data (processing details)

4. How to take out the reports

After the users are trained about the computerized system, working has to shift from manual to computerized working. The process is called ‘Changeover’. The following strategies are followed for changeover of the system.

(i) Direct Changeover: This is the complete replacement of the old system by the new system. It is a risky approach and requires comprehensive system testing and training.

(ii) Parallel run: In parallel run both the systems, i.e., computerized and manual, are executed simultaneously for certain defined period. The same data is processed by both the systems. This strategy is less risky but more expensive because of the following:

- Manual results can be compared with the results of the computerized system.
- The operational work is doubled.
- Failure of the computerized system at the early stage does not affect the working of the organization, because the manual system continues to work, as it used to do.

(iii) Pilot run: In this type of run, the new system is run with the data from one or more of the previous periods for the whole or part of the system. The results are compared with the old results of the system. It is less expensive and less risky than parallel run approach. This strategy builds the confidence and the errors are traced easily without affecting the operations. The documentation of the system is also one of the most important activities in the system development life cycle. This ensures the continuity of the system. There are generally two types of documentation prepared for any system. These are:

1. User or Operator Documentation
2. System Documentation

The user documentation is a complete description of the system from the users point of view detailing how to use or operate the system. It also includes the major error messages likely to be encountered by the users. The system documentation contains the details of system design, programs, their coding, system flow, data dictionary, process description, etc. This helps to understand the system and permit changes to be made in the existing system to satisfy new user needs.

(i) Maintenance

Maintenance is necessary to eliminate errors in the system during its working life and to tune the system to any variations in its working environments. It has been seen that there are always some errors found in the systems that must be noted and corrected. It also means the review of the system from time to time. The review of the system is done for:

- knowing the full capabilities of the system

- knowing the required changes or the additional requirements
- studying the performance.

If a major change to a system is needed, a new project may have to be set up to carry out the change. The new project will then proceed through all the above life cycle phases.

Self Assessment Exercise

i. What is a system?
ii. Explain system life cycle

4.0 Conclusion

The interdependent and connectivity of a system gives it an overwhelming function to perform. As explained, it represents a complete natural system like the human body. Therefore it must be properly maintained for optimal performance.

5.0 Summary

In this unit a systematic approach to solve any given problem is explained. Phases of system such as preliminary system study, detailed system study, system analysis, design, coding, testing, implementation and maintenance are explained. Computer based systems are defined. System development life cycle is discussed in detail. The different phases of the development of system are explained in detail.

6.0 Tutor Marked Assignment.

1. What is System Analysis?
2. With the aid of a diagram, discuss the phases therein in a system development life cycle

7.0 References/ Further Reading

Barwise, J. and Etchemendy. J. (2001). "Computers, Visualization, and the Nature of Reasoning." Accessible in PDF format via *http://morpheus.hartford.edu/~anderson/*

Bush, V. (1945). As We May Think. *Atlantic Monthly*. July. 101-108. *Design Studies.* January. Available in PDF format via *http://morpheus.hartford.edu/~anderson.*

Erlandson, D. A. (1993). *Doing Naturalistic Inquiry: a Guide to Methods*. Newbury Park: Sage.

Gross, M. D. (1996). "The Electronic Cocktail Napkin - Computer Support for Working with Diagrams,"

Mahon, B., Hourican, R. and Gilchrist, A. (2001). *Research into Information Architecture: The roles of software, taxonomies and people*, London, TFPL.

Narayanan, H. (2001). "Introduction to Diagrammatic Reasoning." *http://morpheus.hartford.edu/~anderson/*

Nitecki, J. Z. (1998). *The Nitecki Trilogy*. *http://venus.twu.edu/library/Nitecki* (accessed 08 October 98).

Schrage, M. (1990). *Shared Minds: the New Technologies of Collaboration*. New York: Random.

Unit 4
Information System Security: A Guide to the Use of Water Quality Management Principles I

Contents

1.0 Introduction

In the last decade of this age of information, a shift in awareness of the role of monitoring and information has become apparent. In the past, monitoring originated from the greater scientific ideal that underpins our quest for knowledge. The consequence, especially in advanced countries, is that monitoring is frequently, if not implicitly, linked to scientific investigation. Water quality monitoring, world-wide, tends to suffer from a chronic failure to establish meaningful programme objectives. In addition, it has become recognized that many western countries suffer from a "data rich, but information poor" syndrome. The responsible organizations acknowledge that they have collected many data, but are unable to answer the basic questions of those using the water. As a consequence, in many countries, data gathering programmes are considered expendable, and are being reduced or even eliminated because there is no clear view of the information product and of the cost-efficiency of monitoring. In recent years there has been an increasing consensus of opinion that information is meant for action, decision-making and use. Data that do not lead to management action, or for which a use cannot be stated explicitly, are being labeled increasingly as "not needed". Regardless of the purpose of monitoring water, one theme runs constantly through all discussions about monitoring system design, i.e. how can monitoring be more cost effective?

2.0 Objectives
Students are expected to know the relevance and role of monitoring and information needs in water management.

3.0 Main body

In general, information is the basis for any management and control. Water management activities are not excluded from this general statement. Management measures not based

on adequate and reliable information are, principally, unaccountable. There is, therefore, a profound need for effective information that is suitable for such use. As a consequence the development of accountable information systems is receiving much emphasis. Effective monitoring programmes are, increasingly, "tailor-made".

Table 1. Different categories of uses of water resources

Category	Major uses
Category 1: Uses without quality standards	Transport system (water, wastewater, shipping) Mineral extraction (sand, gravel, natural gas, oil) Power generation (hydropower dams)
Category 2: Uses with defined quality standards	Process/cooling water in industry Irrigation in agriculture Fisheries Recreation and tourism Domestic water supply
Category 3: "Use" with "undisturbed" quality	Ecosystem functioning

The importance of integration

Information needs for water pollution control can only be defined from within the overall context of water resources management. By considering the various influences and aspects involved in water resources management today, it is possible to identify some fundamental information needs. Some relevant aspects of water resources management are highlighted briefly below.

Functions and use

Various functions and uses of water bodies, whether in relation to human activities or ecological functioning (Table 1), can be identified from existing policy frameworks, international and regional conventions and strategic action plans for river basins and seas. These specify divers requirements for water quality. Uses may compete or even conflict, especially in situations of water scarcity and deteriorating quality. In addition, functions and uses can be affected by human activities in both positive and negative ways (Figure 1). Chemical water quality issues that have given rise to conflicts between water uses in industrialized countries are summarized in Figure 2.

Figure 1.
Interactions between human activities and functions and uses of water resources

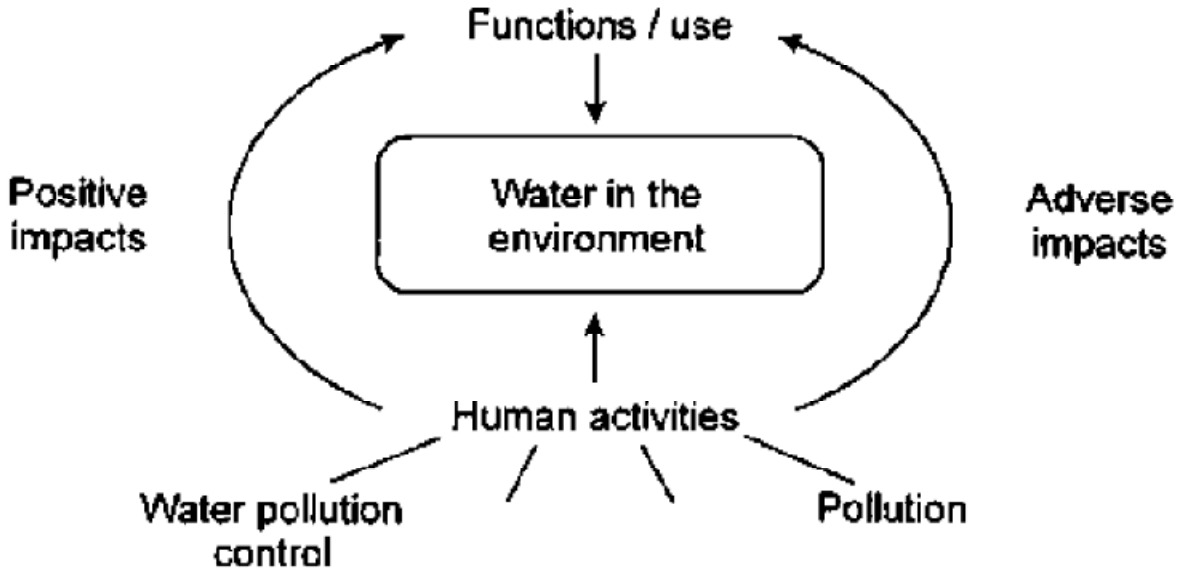
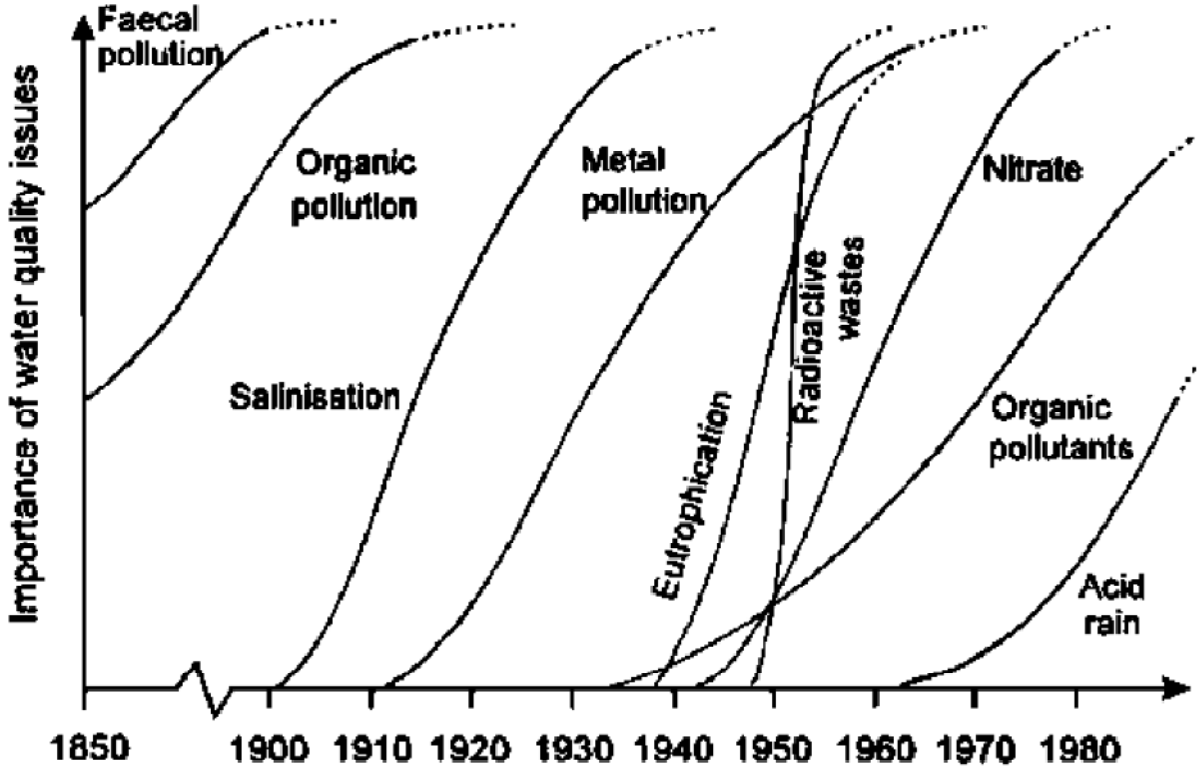


Figure 2.
The sequence of water quality issues arising in industrialised countries (After Meybeck and Helmer, 1989)



Multi-functional approach
An integrated approach tries to find the balance between all desired uses, including ecosystem functioning. A multi-functional approach allows a hierarchy to be introduced to the uses. It allows flexibility in the application of water resources management policies at different levels of development and allows for prioritization in time. This could be important for those countries where basic needs, such as supply of healthy drinking water, are so urgent that other uses must take a lower priority, or for countries where water resources have become deteriorated to such an extent that uses with stricter water quality needs can only be restored gradually over a long period of time and according to their priority. The concept of integrated water management became widely adopted in the 1980s, and as a result the functions and uses of water bodies, their problems and threats, and the effects of water management measures, as well as the information needs to manage this complexity, are being viewed increasingly in an ecosystem context. The focus is now on the behaviour of water in the environment. Instead of breaking the environment into manageable parts, managers are leaving their restricted, traditional disciplines and taking a broad "systems" perspective of water quality management and monitoring.

Various disciplines
Knowledge on various disciplines is required because the functions and uses of water resources may be related to physico-chemical, biological, morphological, hydrological and ecological features. The nature of water pollution issues and the effects of controlling measures do not allow a divided approach; they have to be characterized in an integrated way. For the same reason, information needs also require an integrated approach.

Appropriate media
Various media, such as the water itself, suspended matter, sediments and biota are integrated elements of a water body. Information needs are also concerned with appropriate media, wherever these media provide information that is considered to be characteristic for functions, problems and control measures. Interactions of water resources with air and soil demand the same approach.

Multiple sources
Multiple sources of water pollution require an integrated, balanced and site specific approach. If water pollution is dominated by well-defined point sources, monitoring of the discharged effluents may be the best approach. Generally, however, point sources are numerous and not well defined. In addition, diffuse sources are forming a substantial and growing aspect of water pollution problems. Knowledge of the relative contribution of different sources (agriculture, households, industries, aerial deposits) is often important to verify the effectiveness of control measures.

Table 2.

Differences in the emission-based and the water quality-based approaches to water pollution control

Management aspect	Emission-based approaches	Water quality based approaches
Effluent limits	No site-specific load	Site-specific concentrations
Required treatment techniques	Based on intrinsic (toxic) properties of chemicals in effluent; or technology based	Based on water quality criteria or preventing toxic effects in the effluent receiving water
Data requirements	Basic chemical and ecotoxicological data	Basic chemical and ecotoxicological data. Physical, chemical and biological characteristics for the receiving water and the fate of discharged chemicals
Monitoring	Effluent	Receiving water
Competition	Equality for the law	Inequality
Practice	May tend to worst case approach in general, but may underestimate effects of discharges in specific situations	May tend to dilution as a solution in general, but stricter standards are possible when effects are intolerable in specific situations

Source: Stortelder and Van de Guchte, 1995

Approaches in water pollution control

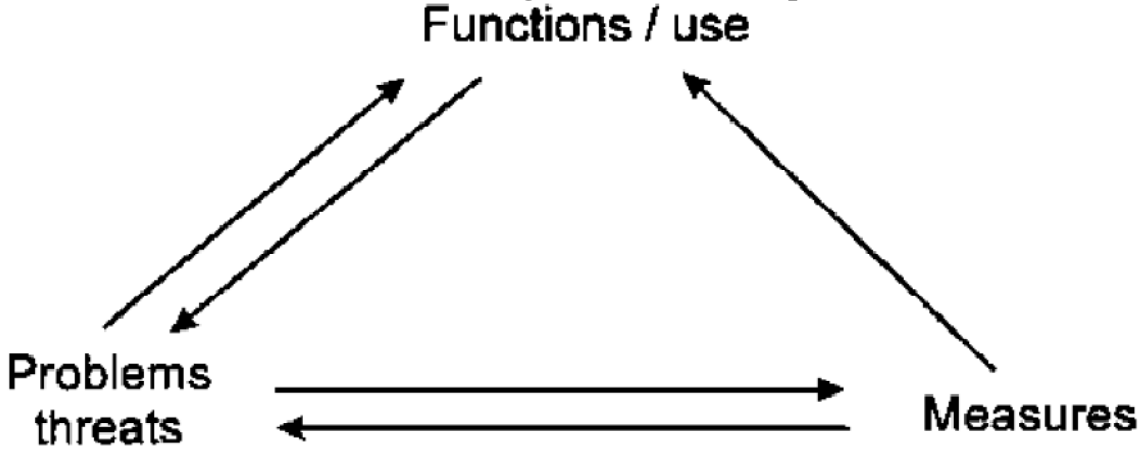
There are two approaches to water pollution control: the emission-based approach and the water quality-based approach. The differences between these approaches result from the systems applied for limiting discharge and in the charging mechanisms. However, these differences are also reflected in the strategies taken for hazard assessment and the monitoring of discharges to water, i.e. whether it is focused on the effluents or on the receiving water; both have their advantages and disadvantages (Table 2). A combined approach can make optimal use of the advantages.

Watershed management

Ecosystems are not restricted to boundaries defined by humans, such as between local governments or countries. Consequently, integrated watershed management is becoming more common. The Convention on Protection and Use of Transboundary Watercourses and International Lakes, Helsinki (UNECE, 1992) underlines the need for an integrated watershed approach in water management and for adequate monitoring and assessment of transboundary waters.

Figure 3.

Core elements in water management and water pollution control



Institutional collaboration

In many countries the responsibility for collecting water information is divided between, for example, different ministries, executive boards, and agencies. This approach risks duplication and a lack of harmonization, and prevents an integrated approach. Often, responsibilities for water resources management and water pollution control rest with different ministries and with different governmental levels (federal, regional, local). The establishment of collaborative partnerships and the co-ordination of monitoring efforts between competing ministries or institutions can greatly enhance the quality of the information obtained and make better use of available resources.

Specifying information needs

Information needs are focused on the three core elements in water management and water pollution control, namely the functions and use of water bodies, the actual problems and threats for future functioning, and the measures undertaken (with their intended responses) to benefit the functions and uses (Figure 3). Monitoring is the principal activity that meets information needs for water pollution control. Models and decision support systems, which are often used in combination with monitoring, are also useful information tools to support decision making. Figure 4 illustrates some of the key components of the environmental management system. Monitoring objectives are set according to the focus of water management and water pollution control activities and according to the issues that are capturing public attention.

Monitoring objectives may be of many kinds, but fall mainly within five basic categories:

1. Assessment of water bodies by regular testing for compliance with standards that have been set to define requirements for various functions and uses of the water body concerned.

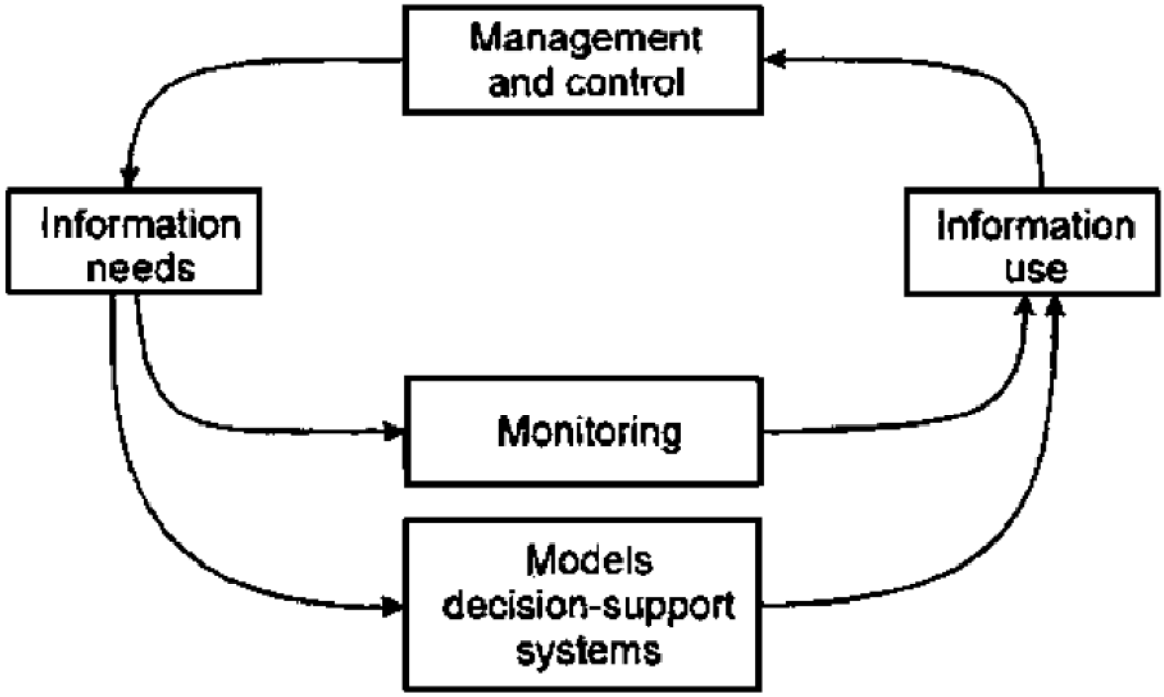
2. Testing for compliance with discharge permits or for setting of levies.

3. Verification of the effectiveness of pollution control strategies, i.e. by obtaining information on the degree of implementation of measures and by detection of long-term trends in concentrations and loads.

4. Early warning of adverse impact for intended water uses, e.g. in case of accidental pollution.

5. Increasing awareness of water quality issues by in-depth investigations, for example by surveys investigating the occurrence of substances that are potentially harmful. Surveys provide insight into many information needs for operational water management.

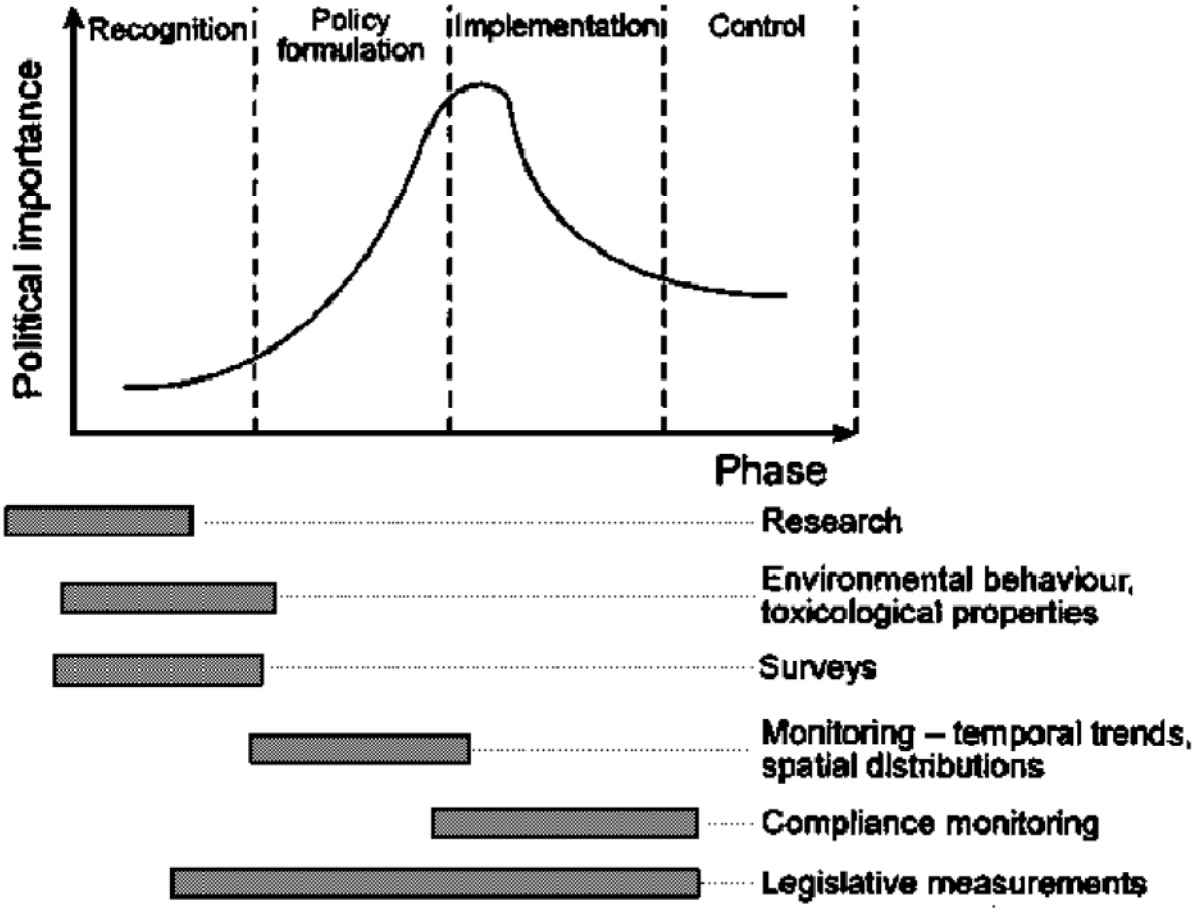
Figure 4
Components of environmental management information systems



A monitoring objective, once defined, identifies the target audience. It makes clear who will be the users of the information and why the information is needed. It also identifies the field of management and the nature of the decision-making for which the information will be needed. It should be recognised that the detection of trends, in itself, is not a monitoring objective but a type of monitoring. Only when the intended use of the trend information is specified can it be considered to be an objective. Once objectives have been set it is important to identify the information that is needed to support the specified objective. The content and level of detail of the information required depends upon the phase of the policy life cycle (Figure 5). In the first phase, research and surveys may

identify priority pollution problems and the elements of the ecosystem that are appropriate indicators. Policies will be implemented for these. In the second and third phases, feedback on the effectiveness of the measures taken is obtained by assessing spatial distributions and temporal trends. Contaminants may endanger human health by affecting aquatic resources, such as drinking water, and therefore specific monitoring programmes may be initiated to check, on a regular basis, the suitability of such resources. Legislation may also prescribe measurements required for certain decision-making processes, such as the disposal of contaminated dredged material. In the last phase, monitoring may be continued, although with a different design, to verify that control is maintained. The associated information needs change with the respective policy phases.

Figure 5
The policy life cycle and typical measurement activities applied in the respective phases



Decision-makers have to decide upon the contents and performance of their desired information products. They are the users of the information (for management and control action) and they have to account for their activities to the public. Specification of

information needs is a challenging task which requires that the decision-making processes of information users are formulated in advance. Various aspects of the information product must be specified, such as:

• The water quality assessment needs and the methods to be applied have to be defined, putting an emphasis on the development of a strategy of assessment rather than on a simple inventory of arbitrary needs for the measurement of substances.

• The methods for reporting and presenting the information product must be considered; these are closely related to the assessment methods applied. Visualized, aggregated information (such as indexes) is often much more effective (and therefore more appreciated) than bulky reports.

• Appropriate monitoring variables have to be selected. Selected variables should be indicators that characterize, adequately, the polluting effluent discharge or that are representative for the functions and uses of water bodies, for water quality issues or for testing the effectiveness of pollution control measures.

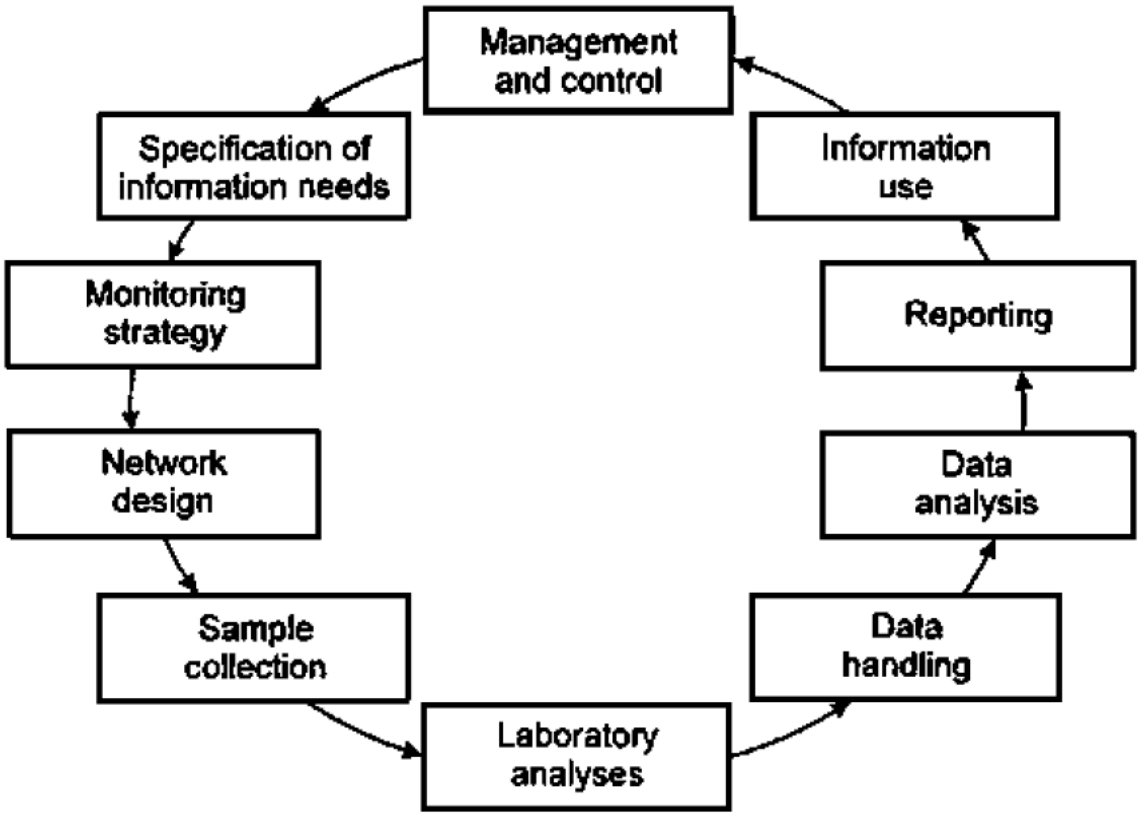
• Relevant margins of information have to be considered. To assess the effectiveness of the information product, the information needs have to be quantified; for example, what level of detail is relevant for decision-making? Such margins have to be specified for each monitoring variable. A relevant margin can be defined as "the information margin that the information-user considers important".

Information needs must be specified such that they enable design criteria for the various elements of the information system to be derived. Specified, relevant margins are a strong tool for network design. With these, sampling frequencies and the density of the network can be optimized, especially if reliable time-series of measurements are available. Relevant margins highlight the detail required in the presentation. Decisions on the development of more accurate analytical methods should be related to relevant margins or threshold values in water quality. However, the latter should be related critically to cost-effectiveness.

In general, a monitoring and information system can be considered as a chain of activities (Figure 6). Essentially, the chain is closed with the management and control action of the decision-maker, whereas past schemes have shown a more top-down sequence of a restricted number of activities, starting with a sampling network chosen arbitrarily and ending up with the production of a set of data. Building an accountable information system requires that the activities in the chain are designed sequentially, starting from the specified information needs. While monitoring is continuing, information needs are also evolving. This has already been illustrated by the policy life cycle in Figure 5. In time, there will be developments in management and control, and targets may be reached or policies may change, implying that the monitoring strategy may need to be adapted.

Dynamic information needs require a regular reappraisal of the information system; it is essential to add, to cancel, to revise and to bring the concept up to date. In order to visualise this the circle of Figure 6 may be modified to a spiral (Cofino, 1994), reflecting the ongoing nature of the monitoring and incorporating the feedback mechanism.

Figure 6: Chain of activities in an information system



Self Assessment Exercise

1. Monitoring and information system can be considered as a chain of activities. Discuss

2. What are the three core elements in water management and water pollution control?

4.0 Conclusion

The relevance and the need for an integrated watershed approach in water management cannot be over emphasized if man is to maximally enjoy the benefit of the ecosystem in all aspect of life, from basic usage to industrial and manufacturing purpose.

5.0 Summary

The importance of information needs for water pollution control, and the interactions between human activities, functions and uses of water resources were clearly stated. In doing so various approaches to the management of decisions regarding pollution control were highlighted such as the Components of environmental management information systems, Chain of activities in an information system, Monitoring objectives among others as necessary in decision management process.

6.0 Tutor Marked Assignment

What are the Components of environmental management information systems?

7.0 References/ Further Reading

Adriaanse, M., Van de Kraats, J., Stoks, P.G. and Ward, R.C. (1995) Conclusions monitoring tailor-made. In: M. Adriaanse, J. Van de Kraats, P.G. Stoks and R.C. Ward [Eds] *Proceedings of the International Workshop Monitoring Tailor-made.* Institute for Inland Water Management and Waste Water Treatment (RIZA), Lelystad, The Netherlands.

Bartram, J. and Ballance, R. (1996). *Water Quality Monitoring. A Practical Guide to the Design and Implementation of Freshwater Quality Studies and Monitoring Programmes.* Published on behalf of UNEP and WHO by Chapman & Hall, London.

Chapman D. and Jackson, J. (1996). Biological monitoring. In: J. Bartram and R. Balance [Eds] *Water Quality Monitoring. A Practical Guide to the Design and Implementation of Freshwater Quality Studies and Monitoring Programmes.* Published on behalf of UNEP and WHO by Chapman & Hall, London, 263-302.

Cofino, W.P. (1995). Quality management of monitoring programmes. In: M. Adriaanse, J. Van de Kraats, P.G. Stoks and R.C. Ward [Eds] *Proceedings of the International Workshop Monitoring Tailor-made.* Institute for Inland Water Management and Waste Water Treatment (RIZA), Lelystad, The Netherlands.

Demayo, A. and Steel, A. (1996). Data handling and presentation. In: D. Chapman [Ed.] *Water Quality Assessments. A Guide to the Use of Biota, Sediments and Water in Environmental Monitoring.* Second Edition. Published on behalf of UNESCO, WHO and UNEP by Chapman & Hall, London, 511-612.

Dogterom, J. and Buijs P.H.L. (1995). *Concepts for Indicator Application in River Basin Management.* Report 95.01. International Centre of Water Studies (ICWS), Amsterdam.

Dubelaar, G.B.J., Balfoort, H.W. and Hofstraat, H.W. (1990). Automatic identification of phytoplankton. In: *North Sea Pollution: Technical Strategies for Improvement.* N.V.A. Rijswijk, The Netherlands, 539-542.

EPDRB (EPDRB) (1994). *Strategic Action Plan (SAP) for the Danube River Basin 1995-2005.* Task Force for the Environmental Programme for the Danube River Basin, Brussels.

Friedrich, G., Chapman, D. and Beim, A. (1996). The use of biological material. In: D. Chapman [Ed.] *Water Quality Assessments. A Guide to the Use of Biota, Sediments and Water in Environmental Monitoring.* Second Edition. Published on behalf of UNESCO, WHO and UNEP by Chapman & Hall, London, 175-242.

Griffiths, I.M. and Reeder, T.N. (1992). Automatic river quality monitoring systems operated by the National Rivers Authority - Thames Region, UK. *Eur. Wat. Poll. Cont.*, 2(2), 523-30.

Stortelder, P.B.M. and Van de Guchte, C. (1995). Hazard assessment and Monitoring of discharges to water: concepts and trends. *Eur. Wat. Poll. Cont.*, 5(5).

UNECE (1992). *Convention on the Protection and Use of Transboundary Watercourses and International Lakes.* United Nations Economic Commission for Europe, Geneva.

Unit 5
Information System Security: A Guide to the Use of Water Quality Management Principles II

Contents

1.0 Introduction

The objective of an information system for water pollution control is to provide and to disseminate information about water quality conditions and pollution loads in order to fulfil the user-defined information needs. Information systems can be based either on paper reports circulated in defined pathways, or on a purely computerized form in which all information and data are stored and retrieved electronically.

2.0 Objectives

Students are expected to know:

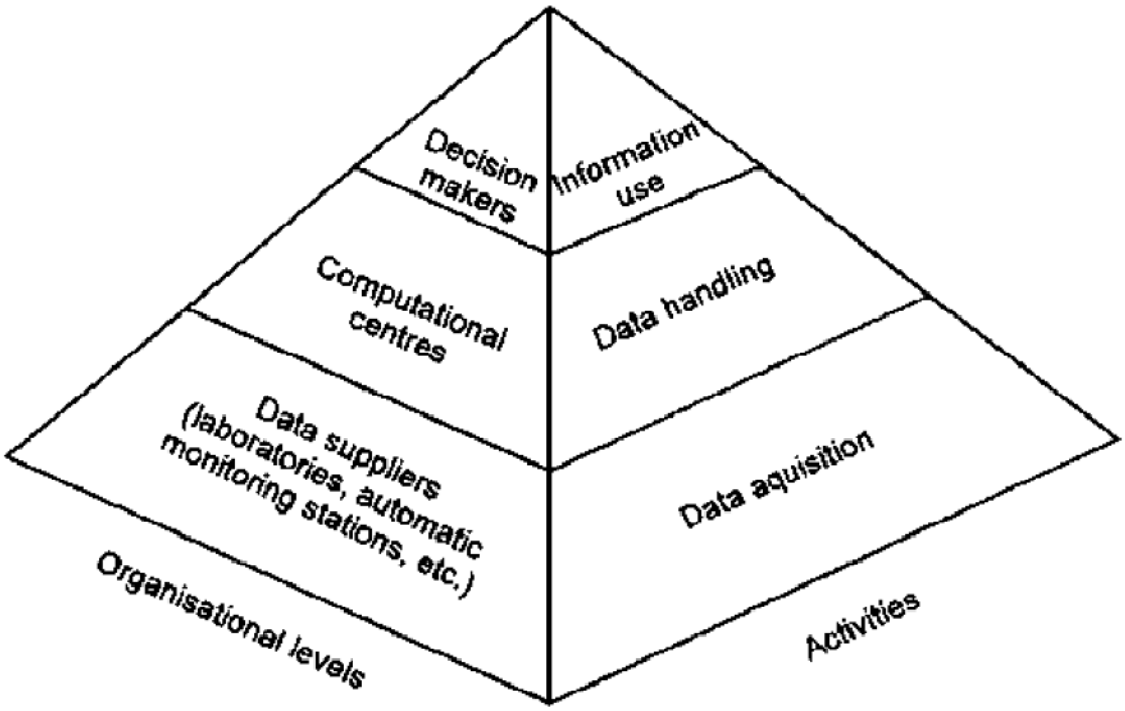
1. objective of an information system for water pollution and
2. types of data and information tool to be processed in an information system

3.0 Main body

In practice, most information systems are a combination of these. However, given the availability of powerful and inexpensive hardware and software, it is now almost unthinkable to design an information system without making use of computers for data management and analysis. The main types of data to be processed in an information system are:

• Data on the nature of the water bodies (size and availability of water resources, water quality and function, and structure of the ecosystem).
• Data on human activities polluting the water bodies (primarily domestic wastewater and solid waste, industrial activities, agriculture and transport).
• Data on the physical environment (e.g. topography, geology, climate, hydrology).

Figure 1: Information "pyramid" showing information system activities and their corresponding organizational levels



Such data must be drawn from networks of national, regional and local monitoring stations on water quality and on pollution sources. The flow of data in information systems must be well defined in order to fulfill the requirements of users and the overall demand for reliability. Data flow is considered in three directions, upwards, downwards and horizontally. Upward flow of information from lower to higher organizational structures reduces the amount of detail but enhances the information value through the interpretation of the data. Downward flow is important for the purpose of communicating decisions in relation to national standards and policies, and also to make a feedback to those involved in data acquisition and data-handling within the information system. Horizontal flow, through data sharing between organizations, is essential for developing an integrated approach to environmental monitoring and management and to make efficient use of data that are often collected and stored in a large number of institutions.

The vertical flow of information can often be described as a three-tiered system with respect to the organizational levels and the activities performed at each level. This is illustrated in the "information pyramid" (Figure 1) which reflects the large number of data at the lowest level which, as they reach higher levels of the triangle, become less detailed but of greater information value. The first level is responsible for primary data acquisition through monitoring, data validation and storage of data. Often the data will be dynamic, such as measurements and analyses and, typically, will be used locally (such as

for compliance control). It is very important to implement basic quality assurance and control systems for all procedures generating primary data because the data generated at this level will influence the result of data analysis, reports and decisions also taken at other levels. Data handling (the second level) is typically carried out at computational centres and can be organized thematically, such as on water quality in rivers, lakes or groundwaters or by pollution source, for example municipal and industrial wastewater, non-point pollution from agriculture. Computational centres can also be divided geographically according to river basins or to administrative boundaries, i.e. to local or regional level. These centres have the primary task of converting data into information. They are, therefore, the users of primary data from the data acquisition level as well as being the service centres producing the required information. Typically these centres use and maintain adequate graphical and statistical tools, forecasting tools (e.g. models) and presentation and reporting tools.

In addition, they often maintain data of a more static nature, such as geographical data, and they may also be responsible for primary data acquisition within their specific area of responsibility. The third level (information use) is made up of the decision-making authorities who are the end-users of the information produced. At this level, information is used for checking and correcting the policies and management procedures applied. However, this level is also responsible for the final generation of the information disseminated to the public and to other interested parties, such as private sector and international bodies and organisations. As such, this level may have its own tools for integrating the information on the water environment with information from other media and sectors.

Data acquisition

Data acquisition deals with the generation and storage of data from monitoring activities. Data should be stored to ensure that they maintain accuracy and to allow easy access, retrieval and manipulation. The volume of data to be acquired and stored is dictated by the size and level of ambition of the monitoring network. For small volumes of data, manual systems may be used efficiently to store and retrieve data, produce time series plots and to perform simple statistical analysis. Nevertheless, a system based on microcomputers, and using simple systems like spreadsheets, may substantially improve data handling capacity, simultaneously enabling basic statistical and graphical analyses that are straightforward and easy to perform. For larger volumes of data, a generalized data storage system, based on a relational database, will provide more powerful data management capabilities. In addition to being used for storage and retrieval of data, special programmes can be written for such systems to automate data entry, analysis and generation of reports.

The following general requirements for storing data in databases can be identified;

- Data must be stored and retrieved unambiguously.
- Software must be portable.

• Software must be easy to use.
• Protection against wilful or accidental damage must be assured.
• Unambiguous output must be assured.
• Flexible enquiry and reporting should be possible.

Data handling

Data handling covers the analysis and transformation of data into information. Tools for this are described in more detail. The preparation of reports and the dissemination of information is another important aspect of an information system. Issues, such as for whom the reports are intended, at what frequencies should they be generated, and the level of detail of each report, should be clarified and the reporting systems should be planned as an integral part of the information system. Reports containing results from routine analyses of data collected from a monitoring programme (i.e. daily, weekly, monthly, quarterly or yearly), and that present developments in water quality or pollution load since the preceding monitoring period should be prepared using a fixed format. The reporting can then be automated using a customised data management system. Other types of report present information generated on the basis of data from various pollution sources and locations and analysed by means of advanced tools such as models and geographical information systems (GIS). These types of report are particularly useful in water pollution control because they focus on water quality as well as on pollution sources. Some examples are:

• *State of the environment (SOE) reports.* These are environmental summary assessments used to inform decision makers, environmental organisations, scientists and the public about the quality of the environment. Such reports normally include the state of the environment; changes and trends in the state of the environment; links between human and environmental health and human activities, including the economy; and the actions taken by society to protect and to restore environmental quality.

• *Environmental indicator reports.* These are considered to be an effective way of communicating with the public, amongst others, and of presenting information about the development of a number of indicators over time and space. Environmental indicators are sets of data selected and derived from the monitoring programme and other sources, as well as from data bases containing statistical information, for example, on economy, demography, socio-economics. For pollution control in rivers, examples of useful indicators are dissolved oxygen, biochemical oxygen demand (BOD), nitrate, uses and extent of available water resources, degree of wastewater treatment, use of nitrogenous fertilizers and land-use changes, accidents with environmental consequences. An example of an indicator report for the state of Danish rivers is given in Figure 2.

Use and dissemination of information

Use of information is the third and highest level of the information system. At this level the information, mostly in the form of reports, can be used to support decision makers.

New approaches to water pollution control put much emphasis on the active participation of the public, as well as industries. It will, therefore, be increasingly important to disseminate to these parties relevant and easily understandable information about the state of the environment, as well as the extent to which environmental policies and private and public environmental investments are improving the state of the environment. Other activities can be used in addition to the dissemination of reports and may help to raise the environmental awareness of governments, sectoral ministries and administration, as well as the private and public sector. Examples of these activities include seminars, meetings and public hearings held in connection with the launching of significant reports, such as the state of the environment report or environmental indicator reports.

From data to information tools

To avoid the "data rich but information poor" syndrome, data analysis, information generation and reporting should be given the same attention as the generation of the data themselves. Water pollution control requires access to statistical, graphical and modelling tools for analysis and interpretation of data. Theoretically, most of these analyses can be performed manually, although this approach is often so time consuming that for large data sets and complex data treatment methods it excludes the generation of the type of information required.

Graphical information

Data analyzed and presented using graphical methods is probably the most useful approach for conveying information to a wide variety of information users, both technical and non-technical. Graphical analyses are easy to perform, the graphs are easy to construct and the information value is high when graphs are properly presented. The types of information that can be presented most effectively by graphical methods are:

- Time series (temporal variation).
- Seasonal data (temporal variation).
- Water quality at geographic locations (spatial variations).
- Pollution loads at geographic locations.
- Statistical summaries of water quality characteristics.
- Correlations between variables.
- Spatial and temporal comparisons of water quality variables.

Figure 2. Percentage distribution of the types of quality objectives adopted for Danish water courses (according to the regional plan maps of the countries).

Widely used methods include time series graphs and graphs which may be used to give a visual indication of data distribution (e.g. box and whisker plots) and to indicate how distribution changes over time or between locations.

Statistical information

Statistical information is the most useful treatment of data for making quantitative decisions, such as whether water quality is improving or getting worse over time, or whether the installation of a wastewater treatment plant has been effective, or whether water quality criteria or emission standards are being complied with. Statistics can also be used to summarize water quality and emission data into simpler and more understandable forms, such as the mean and median (Demayo and Steel, 1996).

Another important application of statistics, in relation to water pollution control, is the transformation of data to give an understanding of the average and extremes of water quality conditions, and also the changes or trends that may be occurring. Statistical methods to provide this kind of information can be classified as graphical. Standard software packages exist for most statistical methods. An explanation of the use of statistical methods, together with some examples, is available in Demayo and Steel (1996).

Water quality indices and classes

A water quality index is obtained by aggregating several water quality measurements into a single number. Indices are, therefore, simplified expressions of a complex set of variables. They have proved to be very efficient in communicating water quality information to decision makers and to the public. Different water quality indices are in use around the world and among the best known are biological indices, such as the

Saprobic Index. Many countries world-wide use a classification system for the water quality of rivers, dividing the rivers into four (or more) classes of quality, ranging from bad to good. Such systems are mostly based on the use of biological indices, sometime in combination with chemical indices.

In Denmark, for example, quality objectives for the condition of Danish water courses have been adopted and approved as binding directives in the regional plans of the county councils. These quality objectives for water courses are laid down according to the physical and flow conditions of the water course and to the water quality conditions accepted by the authorities responsible for the quality of the water bodies. Table 1 shows these quality objectives and Figure 2 shows the percentage distribution of the types of quality objectives adopted for Danish water courses. Objectives A and B, which apply to more than 75 per cent of the lengths of all water courses, include biological criteria for areas with strengthened objectives or high scientific interest (A) or general objectives for areas sustaining a fish population (B) (DEPA, 1991). Water quality indices and classifications should not be the only method used for analysing and reporting data from a water quality monitoring system, because it may not be possible to determine less obvious trends in water quality and some water quality variables may change dramatically without affecting the overall classification.

Table 1 Types of quality objectives for Danish water courses

Quality objectives		Maximum Saprobic Index
A	Area with specific scientific interests	II
B_1	Spawning and fry	II
B_2	Salmonid water	II
B_3	Carponides water	II (II-III)

Source: Based on information from the National Agency of Environmental Protection,

Models

Water quality models can be a valuable tool for water management because they can simulate the potential response of the aquatic system to such changes as the addition of organic pollution or nutrients, the increase or decrease in nutrient levels, or water abstraction rates and changes in sewage treatment operations. The potential effects of toxic chemicals can also be estimated using models. Mathematical models are, therefore, useful tools for water quality management because they enable:

a. The forecasting of impacts of the development of water bodies.
b. The linking of data on pollution loads with data on water quality.
c. The provision of information for policy analysis and testing.
d. The prediction of propagation of peaks of pollution for early warning purposes.
e. The enhancement of network design.

In addition, and equally important, they enable a better understanding of complex water quality processes and the identification of important variables in particular aquatic systems. Obtaining the data necessary for construction or verification of models may require additional surveys together with data from the monitoring programme. If models are to be used routinely in the management of water quality, it is also important to verify them and for the model user to be aware of the limitations of the models. The development of models into combined systems linking physical, chemical and biological processes has enabled a better understanding and modelling of chemical and biochemical processes and behavioural reactions. It has also shown how such processes interact with basic physical processes (i.e. flow, advection and dispersion). These types of models are gradually being used for water quality management. Several models have been dedicated for specific water quality management purposes such as environmental impact assessment, pre-investment planning of wastewater treatment facilities, emergency modelling and real-time modeling.

Knowledge-based systems (also called decision support systems) are computer programmes that are potentially capable of identifying unexpected links and relationships based on the knowledge of experts. Knowledge-based systems can be used for network design, data validation and interpretation of spatial data. Knowledge-based systems are

also applicable for managing the complex rules of legislation, regulations or guidelines. In recent years, knowledge-based systems have been introduced for environmental applications. Most of these systems have focused on data-interpretation, although systems have also been developed for sampling strategy; for example, Olivero and Bottrell (1990) developed a sampling strategy for soils and Wehrens *et al.* (1993) reported the design of a decision support system for the sampling of aquatic sediments. Simple knowledge-based systems can provide, for example, the necessary information to decide if, and what, action should be taken when specific pollutant concentrations exceed certain standards. One of the advantages of decision support systems is that they can make the knowledge of a few experts available to many non-experts. Furthermore, developing knowledge-based systems forces experts to make their knowledge explicit and, in this way, new knowledge may be discovered. Knowledge-based systems can also work with incomplete knowledge and uncertainty. The development of knowledge-based systems has only begun recently. Therefore, the lack of experience with their use suggests caution is necessary when first implementing such systems. Possible problems to be considered are:

• The development of knowledge-based systems is time-consuming and, often, expensive.

• The acquisition of knowledge is difficult because the number of experts is small and many experts may never have conceptualized the process by which they reach particular conclusions.

• The adaptation of knowledge-based systems to new situations often requires the assistance of the persons who built the system. Knowledge-based systems can be considered as a branch of artificial intelligence. Another promising branch (recently gaining increased interest) is artificial neural networks. Artificial neural networks are very powerful at pattern recognition in data sets and at dealing with uncertainties in the input data. They are, therefore, especially applicable in situations where expert knowledge cannot easily be made explicit or where considerable variability in input data can occur. The standardization provided by the application of artificial neural networks will lead to improved data interpretation, particularly for biological assessments. Most applications of artificial neural networks are still in an experimental stage although some interesting examples can be found for biological classification of river water quality and the automatic identification of phytoplankton.

Geographical information systems

Data used for water pollution control, such as water quality, hydrology, climate, pollution load, land use and fertilizer application, are often measured in different units and at different temporal and spatial scales. In addition, the data sources are often very diverse (Demayo and Steel, 1996). To obtain information about, for example, spatial extent and causes of water quality problems (such as the effects of land-use practices), computer-based GISs are valuable tools. They can be used for data presentation, analysis and interpretation. Geographical information systems allow the geo-referencing of data,

analysis and display of multiple layers of geographically referenced information and have proven their value in many aspects of water pollution control. For example, they have been used to provide information on:

• Location, spatial distribution and area affected by point-source and non-point source pollution.

• Correlations between land cover and topographic data with environmental variables, such as surface run-off, drainage and drainage basin size.

• Presentation of monitoring and modelling results at a geographic scale.

A typical GIS system consists of:

• A data input system which collects and processes spatial data from, for example, digitized map information, coded aerial photographs and geographically referenced data, such as water quality data.

• A data storage and retrieval system.
• A data manipulation and analysis system which transforms the data into a common form allowing for spatial analysis.
• A data reporting system which displays the data in graphs or maps.

Environmental management support systems
Advanced systems combining databases, GIS and modeling systems into one application are sometime called environmental management support systems. These systems are designed to fulfill a specific purpose, such as the management of water resources and they allow integrated assessments of the effectiveness of environmental policies and planning, such as good agricultural practice and application of best available technology. Such systems require a substantial effort in monitoring and system design, implementation and updating. However, because they may serve as a basis for policy development and assessment for a long period of time, they can be a cost-effective tool for controlling high priority water quality problems.

A system integrating monitoring and modelling of water resources (groundwater as well as surface water) has the following elements:

• A GIS-based database of all relevant spatial data, such as topography, river systems (including drainage), soil types, present water resources and land use, plans and restrictions for future water resources and land use (including, for example, forest planting, quantities and distribution of animal manure, livestock watering permits, water reclamation, wells and permitted abstractions), waste disposals and other point sources, and administrative limits.

• A geological database with all relevant geological and hydrogeological data.

• A time series database including data on climate, run-off, pressure level of groundwater, water quality (surface water as well as groundwater), water reclamation and water abstraction.

• Hydrological and water quality models set up and calibrated to different levels of detail with respect to the type of data and the density of monitoring and modelling network.

Design of monitoring networks and selection of variables

To obtain the necessary focus within a monitoring network for water pollution control, network design should be initiated by surveys to identify potential water quality problems and water uses, and by inventories of pollution sources in order to identify major pollution loads. The objectives of any monitoring activities should first be identified by analysis of the requirements of the users of the data. Examples of specific monitoring objectives are:

• To follow changes (trends) in the input of pollutants to the aquatic environment and in compliance with standards.

• To follow changes (trends) in the quality of the aquatic environment (rivers, lakes and reservoirs) and in the development of water uses.

• To evaluate possible relationships between changes in the quality of the environment and changes in the loads of pollutants and human behaviour, particularly changes in land-use patterns.

• To give overall prognoses of the future quality of water resources and to give assessments of the adequacy of water pollution control measures. The key function of network design is to translate monitoring objectives into guidance as to where, what and when to measure. Network design, therefore, deals with the location of sampling, with sampling frequency and with the selection of water quality variables. Obtaining the necessary information for water pollution control may require the following types of monitoring stations:

• *Baseline stations:* monitoring water quality in rivers and lakes where there is likely to be little or no effect from diffuse or point sources of pollution and that will provide natural, or near-natural, effects and trends.

• *Impact stations:* monitoring both water quality and the transport of pollutants. These are located downstream of present and possible future areas of urbanisation, industry,

agriculture and forests, for example. To protect water intakes, additional monitoring stations can be placed upstream of the intakes.

• *Source monitoring stations:* monitoring water quality and enabling calculation of pollution loads. These are located at major point sources and also in catchments which are primarily influenced by non-point source pollution. An additional requirement for selecting the geographic location of stations for baseline and impact monitoring is that they should be at, or close to, current hydrological recording stations or where the necessary hydrological information can be computed reliably. This is because no meaningful interpretation of analytical results for the assessment of water quality is possible without the corresponding hydrometric data base. All field observations and samples should be associated with appropriate hydrological measurements. Other requirements for selecting station locations include accessibility and ease of sampling, safety for operators and transit time for samples going to the laboratory.

If possible, source monitoring stations should be placed at the outlet of major municipal and industrial wastewater discharges (Nordic Fund for Technology and Industrial Development, 1993). Point source monitoring, which requires substantial personnel resources, should be based preferably on self-monitoring performed by municipalities and industries, in combination with public inspection and control systems. The frequency of monitoring should reflect the variability, as well as the magnitude, of the pollution load, i.e. large volume sources should be monitored more frequently than small volume sources.

If monitoring at an outlet is not possible or the discharge is very small, the pollution load from industries may be calculated from information on the type of production and the actual production capacity using standard emission rates. For discharges from urban areas, loads can be calculated using person equivalents. The validity of the calculated information should be checked against values of pollution transport based on results from impact monitoring stations upstream and downstream of the discharges.

Direct monitoring of pollution loads from non-point sources to the water bodies is not possible. However, an impact monitoring station, located downstream of a catchment dominated primarily by non-point sources, such as agriculture, may be used for the evaluation of trends in loads from these sources (DEPA, 1992). If this is not possible because the catchment contains both point and non-point sources, some evaluation of trends in non-point loads may be achieved by subtracting the load from the point sources (monitored at the relevant point source monitoring station in the catchment) from the values obtained at the downstream impact station.

Additional evaluation of the pollution load from diffuse sources can be obtained from data on land-use, including land-use for agriculture, forestry, urban areas, landfills and waste dumps. The information required in relation to agriculture and forestry includes

animal and livestock production, types of crops, soil types, use of fertilizer (by type and amount), and use of pesticides. Data on population size is appropriate for the evaluation of pollution loads from smaller urban and rural areas where there is no infrastructure for waste-water collection and treatment. To transform this type of data into usable information, tools such as models and GIS are necessary. Where monitoring stations are located in lakes with long retention times, the evaluation of pollution loads may require information from the monitoring of atmospheric deposition of nitrogen, phosphorus and heavy metals, especially in more industrialized areas. The selection of sampling frequencies and variables is usually based on a compromise between average station densities, average sampling frequencies and a restricted number of variables (depending on the character of the industrial and agricultural activities in the catchment together with the financial resources of the monitoring agency). Table 9.4 gives some guidance for the development of a water pollution control programme with different levels of complexity. It should also be recognized that sampling frequency and the number of samples required may have to be adapted in order to allow the necessary statistical analysis (Ward *et al.*, 1990; Demayo and Steel, 1996). An advanced monitoring programme in areas with major industrial and agricultural sources of pollution, including the use of pesticides and chemical fertilizers, requires additional media, such as sediment and biological material in which heavy metals and some hazardous chemicals accumulate, and variables, particularly some heavy metals and specific organic compounds, when compared with pollution control monitoring of municipal wastes or traditional agricultural methods. Some industrial discharges may contain toxic chemicals that can affect aquatic life. The introduction of aquatic toxicity tests, using the effluents from industrial sources, may be an effective way of giving information on toxicity (OECD, 1987).

Monitoring technology

This section gives only a brief summary of types of monitoring technology for water pollution control. The main emphasis is on any additional requirements compared with more basic water quality monitoring, i.e. requirements such as technology for monitoring pollution sources, sampling sediment, biological monitoring and laboratory equipment necessary for advanced analysis of some heavy metals and specific organic chemicals. Further guidance on monitoring technology and laboratory methods is given in the *GEMS/WATER Operational Guide*. (WHO, 1992).

Source monitoring

The volumetric flow rate is particularly important for the determination of pollution loads coming from point sources. Flow should preferably be recorded continuously or, if this is not possible, at least during the period of sampling. Suitable manually-operated equipment for monitoring flow includes a meter linked to a propeller, electromagnetic sensors or even a system using buckets and time recording (the latter can provide a good estimate). Water or effluent samples can be taken manually, using simple equipment such as buckets and bottles, or automatically using vacuum or high speed pumps. Spot-samples, giving the concentration just at the time of sampling, should only be used if

there is no other alternative. Instead, time-proportional or flow-proportional samples should be taken over a period of time (e.g. 24 hours) to give a better estimation of the variation of loads over time.

Variables such as temperature, pH, redox potential, turbidity and concentration of dissolved oxygen may be monitored *in situ,* using hand-held portable meters. For other variables, such as chemical oxygen demand (COD), BOD or nutrients or advanced variables such as heavy metals and specific organic chemicals, the samples have to be transported to and analysed at a laboratory. Such variables are often specified in discharge permits. Discharges from some industrial processes may have an adverse effect on aquatic organisms, as a result of toxic components. This toxicity can be evaluated by different types of biological tests in which the organisms are exposed to the effluent (OECD, 1987). An example of such a method is Microtox, which is an off-line method for measuring acute toxicity using bioluminescent bacteria. The principle of the test, which is standardized in some European countries, is to measure the light production of the bacteria before and after exposure to the wastewater for a defined period of time. The result can be used to estimate if the discharge is likely to affect aquatic life in the water body receiving the discharge. Other tests, which may be more relevant, but also more laborious, are based on the exposure of fish or other organisms known to be abundant in the receiving water body (Friedrich *et al.,* 1996)

Particulate matter sampling and biological monitoring

Monitoring programmes for particulate matter and biological material need careful design. In general, the frequency of sampling is low compared with water sampling. However, the analysis of samples is often more time consuming. Monitoring of particulate matter (suspended or deposited on the bottom) is particularly important because heavy metals and some hazardous organic industrial chemicals and pesticides are associated with the particulate matter and accumulate in deposited sediments; therefore, water samples do not give an accurate representation of the pollution load from such substances. Sampling can be performed with inexpensive grab or core samplers (for bottom sediment) or by filtration or centrifugation of water samples (for suspended material). Chemical analyses can be performed on extracts of the samples. Whereas water quality monitoring provides a picture of the quality of the water at the time of sampling, biological monitoring can give an integrated picture of water quality over the life time of the selected fauna and flora. It is impossible to monitor separately the thousands of chemicals often occurring simultaneously in the environment, but biological methods provide an indication of their combined effects. Consequently, biological monitoring has been introduced into many water quality monitoring systems.

Advanced analysis

Water pollution control of industrial chemicals and pesticides needs more advanced and expensive equipment, and better laboratory infrastructure, than may be found in many ordinary water quality laboratories. Appropriate equipment includes atomic absorption

spectrophotometers (AAS) for heavy metals analysis, gas chromatographs (GC) and liquid chromatographs for organic pollutants (in combination with effective pre-concentration.

Automation of monitoring and information systems

Over the last decade, much has been achieved in the automation of monitoring and automatic transfer of data from the monitoring system into the information system. New developments using sensor technology and telemetry, for example, will probably speed up this process. The following presents a short summary of the main approaches to sampling and analysis.

• Manual or automatic on-site water sampling with subsequent analysis using portable analytic equipment. This approach is primarily of importance for physical and chemical variables, such as pH, temperature, redox potential, conductivity and turbidity, as well as for variables which have to be monitored *in situ* (e.g. dissolved oxygen). New developments in monitoring kits and hand-held instruments for chemical variables will increase the number of variables that can be monitored on-site.

• Manual or automatic on-site water sampling with subsequent transport to central facilities for analysis and further processing. At present this is the most common approach. In some areas, where the transportation time to a laboratory is very long or the road infrastructure is not sufficiently developed, analysis using a mobile laboratory may be feasible.

• On-site measurement (using sensors) and simultaneous on-site analysis. Such methods reduce the operational cost by limiting personnel requirements although they are presently not developed to a sufficient level for widespread use.

• Remote sensing of regional characteristics, such as land use, by satellites or airborne sensors. Such methods have gained much interest in recent years, particularly for applications using GIS.

Early warning is important for cases of accidental pollution of surface water (surface water early warning) and for cases where there is a direct danger from accidental pollution of surface water (effluent early warning). Early warning has two objectives; providing an alarm and detection. Alarms may be used to alert water users and to trigger operation management. They mainly inform water supply undertakings that are treating surface water for potable water supplies. To a lesser extent they may inform all other direct users of the water body, e.g. for animal husbandry, arable farming and industry. Detection systems may be used to trace discharges or to identify operation failures. As a result of timely warnings, intakes and uses of water can be suspended, the spread of the pollutant can sometimes be limited to certain less vulnerable areas by water management

measures (e.g. control of locks/weirs, water distribution), and the continued, perhaps calamitous, discharge can be prevented (specifically for effluent early warning).

In addition to the measurements made by an early warning monitoring system other components play an important role. These components include:

• A communication system, in which warning procedures are defined and through which all those involved in the river basin can be informed quickly.

• A model for the calculation of the transit time of a confirmed accidental pollution from a warning centre or a monitoring station to the place where the water is used or abstracted.

• A toxic substances inventory providing information on the deleterious properties of substances. An adequate early warning system integrates all these components. There have been major developments in early warning systems in the last 20 years

Self Assessment Exercise

a. What is a knowledge-based system?
b. What are the components of a typical GIS system consists of?

4.0 Conclusion

The relevance and the need for an integrated watershed approach in water management cannot be over emphasized if man is to maximally enjoy the benefit of the ecosystem in all aspect of life, from basic usage to industrial and manufacturing purpose.

5.0 Summary

This unit emphasized much on the various ways of data collection regarding water management through new technologies such as the GIS which over the last decade has been of immense benefit to man and his environment. A lot has been achieved in the automation of monitoring and automatic transfer of data from the monitoring system into the information system; worthy of note is the development of the sensor technology and telemetry. The unit made use of examples from the Danish environmental survey.

6.0 Tutor Marked Assignment

a. What are the general requirements for storing data in databases?
b. How can they be identified?
c. Succinctly discuss the idea behind the concept "data rich but information poor" syndrome.

7.0 References/ Further Reading

Bartram, J. and Ballance, R. (1996). *Water Quality Monitoring. A Practical Guide to the Design and Implementation of Freshwater Quality Studies and Monitoring Programmes.* Published on behalf of UNEP and WHO by Chapman & Hall, London.

Chapman D. and Jackson, J. (1996). Biological monitoring. In: J. Bartram and R. Balance [Eds] *Water Quality Monitoring. A Practical Guide to the Design and Implementation of Freshwater Quality Studies and Monitoring Programmes.* Published on behalf of UNEP and WHO by Chapman & Hall, London, 263-302.

Chapman, D. (1996). *Water Quality Assessments. A Guide to the Use of Biota, Sediments and Water in Environmental Monitoring.* Second Edition. Published on behalf of UNESCO, WHO and UNEP by Chapman & Hall, London.

Cofino, W.P. (1995). Quality management of monitoring programmes. In: M. Adriaanse, J. Van de Kraats, P.G. Stoks and R.C. Ward [Eds] *Proceedings of the International Workshop Monitoring Tailor-made.* Institute for Inland Water Management and Waste Water Treatment (RIZA), Lelystad, The Netherlands.

Demayo, A. and Steel, A. (1996). Data handling and presentation. In: D. Chapman [Ed.] *Water Quality Assessments. A Guide to the Use of Biota, Sediments and Water in Environmental Monitoring.* Second Edition. Published on behalf of UNESCO, WHO and

DEPA (1991). *Environmental Impact of Nutrient Emissions in Denmark.* Published on behalf of Danish Ministry of the Environment by Danish Environmental Protection Agency.

DEPA (1992). *Redegørelse fra Miljøstyrelsen - Aquatic Environment Nationwide Monitoring Programme 1993-1997.* No. 3. Published on behalf of Danish Ministry of the Environment by Danish Environmental Protection Agency.

Friedrich, G., Chapman, D. and Beim, A. (1996). The use of biological material. In: D. Chapman [Ed.] *Water Quality Assessments. A Guide to the Use of Biota, Sediments and Water in Environmental Monitoring.* Second Edition. Published on behalf of UNESCO,

OECD (1987). *The Use of Biological Tests for Water Pollution Assessment and Control.* Environment Monographs No. 11. Organisation for Economic Co-operation and Development, Paris.

Olivero, R.A. and Bottrell, D.W. (1990). Expert systems to support environmental sampling, analysis and data validation. In J.M. Hudson [Ed.] *Expert Systems for Environmental Applications.* ACS Symp. Series 431. American Chemical Society, Washington, D.C.
UNEP by Chapman & Hall, London, 511-612.

Ward, R.C., Loftis, J.C. and McBride, G.B. (1990). *Design of Water Quality Monitoring Systems.* Van Nostrand Reinhold, New York.

Wehrens, R., van Hoof, P., Buydens, L., Kateman, G., Vossen, M., Mulder, W.H. and Bakker, T. (1993) Sampling of aquatic sediments. The design of a decision support system and a case study. *Anal. Chim. Acta,* **271**, 11-24.

World Health Organisation (1992). GEMS/WATER Operational Guide. Third edition, Unpublished WHO document GEMS/W.92.1. World Health Organization, Geneva.

Module 2

Unit 1. Ethics of Information Communication Technology (ICT)
Unit 2. Identity and Information Security Integration
Unit 3. Integrating Information Assurance into System Administration
Unit 4. Management Information Systems Usability and Associated Risk
Unit 5. Elevating Information Security to Business Security

UNIT 1
Ethics of Information Communication Technology (ICT)

Contents

1.0 Introduction

Globalization and digital convergence in the emerging knowledge society has raised complex ethical, legal and societal issues. We are faced with complex and difficult questions regarding the freedom of expression, access to information, the right to privacy, intellectual property rights, and cultural diversity. ICT is an instrumental need of all humans for the gathering of information and knowledge, and as such, should be

guaranteed as a basic right to all human beings. All over the world, rights that are already legally recognised are daily being violated, whether in the name of economic advancement, political stability, religious causes, the campaign against terrorism, or for personal greed and interests. Violations of these rights have created new problems in human social systems, such as the digital divide, cybercrime, digital security and privacy concerns, all of which have affected people's lives either directly or indirectly.

2.0 Objectives

At the end of this unit, students should be able to comprehend key Information concerning ethical issues regarding ICT:

3.0 Main body

Information technology is impacting all walks of life all over the world. ICT developments have made possible a transition in information storage, processing, and dissemination, from paper to virtual and from atoms to bits, which are now setting new standards of speed, efficiency, and accuracy in human activities. Computerized databases are extensively used to store all sorts of confidential data of political, social, economic or personal nature to support human activities and bringing various benefits to the society. However, the rapid development of ICT globally also has led to the growth of new forms of national and transnational crimes. These crimes have virtually no boundaries and may affect any country across the globe. Thus, there is a need for awareness, policy formation, and enactment of necessary legislation in all countries for the prevention of computer related crime. Globally, internet and computer-based commerce and communications cut across territorial boundaries, thereby creating a new realm of human activities, and undermining the feasibility and legitimacy of applying laws based on geographic boundaries. The new boundaries, which are manifested in the monitor screens, firewalls, passwords, intruder detection, and virus busters, have created new personalities, groups, organizations, and other new forms of social, economic, and political groupings in the cyber world of bits. Traditional border-based law making and law enforcing authorities find this new environment of cyber boundaries very challenging. Cyber systems across the globe have many different rules governing the behaviour of users. Users are completely free to join or leave any system whose rules they find comfortable or uncomfortable. This flexibility may at times lead to improper user conduct. Also, in the absence of any suitable legal framework, it may be difficult for System Administrators to check on frauds, vandalism or other abuses, which may cause the lives of many online users to be miserable. This situation is alarming because any element of distrust for the internet may lead to people avoiding online transactions, thereby directly affecting the growth of e-commerce. The use or misuse of the internet as a medium of communication may in some situations lead to direct damage to real physical society. Non-imposition of taxes on online transactions may have its destructive effect on physical businesses, and also government revenues. Terrorists may also make use of the web to create conspiracies and violence. Wide and free sharing of ideologies, beliefs, convictions, and opinions

between different cultures might cause physical and emotional stress and confusion that might lead to physical violence.

What is Ethics

In the last decade, dozens of ethics centres and programmes devoted to business ethics, legal ethics, bioethics, medical ethics, engineering ethics, and computer ethics have sprung up. These centres are designed to examine the implications of moral principles and practices in all spheres of human activity on our lives. Ethics can be viewed from two angles, normative and prescriptive. First, ethics refers to well-based standards of right and wrong that prescribe what humans ought to do, usually in terms of rights, obligations, benefits to society, fairness, and specific virtues. Ethics, for example, refers to those standards that impose the reasonable obligations to refrain from rape, stealing, murder, assault, slander, and fraud. Ethical standards also include those that enjoin virtues of honesty, compassion, and loyalty. And, ethical standards include standards relating to rights, such as the right to life, the right to freedom from injury, the right to choose, the right to privacy, and right to freedom of speech and expression. Such standards are adequate standards of ethics because they are supported by consistent and well-founded reasons. Secondly, ethics refers to the study and development of personal ethical standards, as well as community ethics, in terms of behaviour, feelings, laws, and social habits and norms which can deviate from more universal ethical standards. So it is necessary to constantly examine one's standards to ensure that they are reasonable and well-founded. Ethics also means, then, the continuous effort of studying of our own moral beliefs and conduct, and striving to ensure that we, and our community and the institutions we help to shape, live up to standards that are reasonable and solidly-based for the progress of human beings.

Definition

"*Ethics are moral standards that help guide behaviour, actions, and choices*. Ethics are grounded in the notion of responsibility (as free moral agents, individuals, organizations, and societies are responsible for the actions that they take) and accountability (individuals, organizations, and society should be held accountable to others for the consequences of their actions). In most societies, a system of laws codifies the most significant ethical standards and provides a mechanism for holding people, organizations, and even governments accountable." (Laudon, et al, 1996)

ICT Ethics

ICT ethics are not exceptional from the above-mentioned view of ethics. In a world where information and communication technology has come to define how people live and work, and has critically affected culture and values.

ICT Ethical Issues

Analysing and evaluating the impact of a new technology, such as ICT, can be very difficult. ICT does not only involve technological aspects, but also epistemology since

the main component of ICT is information which represents data, information, and knowledge. ICT assists and extends the ability of mankind to capture, store, process, understand, use, create, and disseminate information at a speed and scale which had never been thought possible before. Some of the impact and changes of ICT are obvious, but many are subtle. Benefits and costs need to be studied closely for a nation to progress and improve the quality of life for its citizens. Issues that have arisen from the adoption of ICT, such as the application of automated teller machines (ATM), can be summarized as follows:

- Unemployment

The automation of work has caused creative destruction by eliminating some vocations and creating new ones. How does this affect the employment or unemployment of the work force of a nation?

- Crime

Stolen and counterfeit ATM cards are used to steal millions of dollars each year throughout the world. The anonymity of the machines makes some crimes easier and creates many new types of crimes.

- Loss of privacy

Transactions are transmitted and recorded in databases at banks, hospitals, shopping complexes, and various organizations, in the public or private sector.
The contents of electronic communications and databases can provide important and private information to unauthorised individuals and organizations if they are not securely guarded.

- Errors

Information input into the databases is prone to human and device error. Computer programmes that process the information may contain thousands of errors. These errors can create wrong and misleading information about individuals and organizations. Information and programme errors might result in financial loss, or even the loss of lives.

- Intellectual property

Millions of dollars of software is illegally copied each year all over the world. This phenomenon has a great impact on the software industry. Local and foreign software industries need consumers support all over the world to maintain the progress of technology. Most importantly, for the sake of growth in indigenous ICT innovation and invention, local software industries in Asia-Pacific need local support in protecting their intellectual property rights and investment.

- Freedom of speech and press

How do the constitutional rights of individuals in terms of the freedoms of speech and press apply to electronic media? How seriously do the problems of pornography, harassment, libel, and censorship on the net affect individuals and society? What government initiatives have been used in handling this crisis?

- Digital Divide

How does ICT affect local community life? The increasing use of computers has increased the separation of rich and poor, creating a digital divide between the information "haves" and "have-nots." What subsidies and programmes have been provided by governments to address the issue?

- Professional Ethics

How well trained and ethical are our ICT professionals in dispensing their duties? Faulty and useless systems that cause disasters and hardships to users might be built by incompetent ICT professionals. In dispensing their duties ICT professionals must demonstrate their best practices and standards as set by professional bodies for quality assurance.

UNESCO's Info-Ethics Programme

The development of digital technologies and their application in worldwide information networks are opening vast and new opportunities for efficient access to and use of information by all societies. All nations can fully benefit from these opportunities on the condition that they meet the challenges posed by these information and communication technologies. Thus, UNESCO's Info-Ethics Programme was established for the principal objective of reaffirming the importance of universal access to information in the public domain, and to define ways that this can be achieved and maintained in the Global Information Infrastructure. It seeks to address the areas of ethical, legal and societal challenges of cyberspace, as well as privacy and security concerns in cyberspace. It aims to encourage international cooperation in the following aspects: (http://www.unesco.org/webworld/public_domain/legal.html)

- Promotion of the principles of equality, justice and mutual respect in the emerging Information Society;

- Identification of major ethical issues in the production, access, dissemination, preservation and use of information in the electronic environment; and

- Provision of assistance to Member States in the formulation of strategies and policies on these issues.

Self Assessment Exercise

List and discuss the relevant Ethical Issues in ICT.

4.0 Conclusion

The underprivileged need to be made aware of the importance of ICT. They need to be given access to the infrastructure and services available, and provided with the skills for using ICT, in order to establish their presence in the world, and, ultimately, be able to gain the benefits provided by ICT positively for wealth creation through e-commerce and the service industries. This might help in achieving the millennium development goal of halving global poverty by 2015.

5.0 Summary

This unit takes a careful look at ICT as it assists and extends the ability of mankind to capture, store, process, understand, use, create, and disseminate information at a speed and scale which had never been thought possible before, however not without some ethical issues affecting cultures and values in society. The writers wish to inform that there are other related ethical issues and definitions on ICT security. Other issues not discussed here can easily be found on the internet and other scholarly materials recommended. In case students have any question regarding any aspect of this study for assistance please contact your tutorial facilitator.

6.0 Tutor Marked Assignment

The impact of ICT, as a technology can be very difficult. Explain this in terms of analyses and evaluation.

.

7.0 References/ Further Reading

Broadhurst, R. (2002). E-commerce & Cybercrime: issues, problems & prevention. Asia-Pacific Conference on Cybercrime and Information Security, Seoul, Republic of Korea, 11-13 November 2002.

Computer SecurityInstitute. CSI. (2003). CSI/FBI Computer Crime and Security Survey.

Johnson, D.G. (1994). *Computer Ethics,* second edition; Englewood Cliffs, NJ, Prentice Hall.

Laudon, K. 1995. “Ethical Concepts and Information Technology,” Communications of the ACM, December 1995 p 33-40.

Laudon, K.C., Traver, C.G. and Laudon J.P. (1996). Information Technology and Society, Pp.513.

Leveraging Effective ICT Strategies For Sustainable Development. A Regional Initiative for Information and Communications Technology Strategies (RIFICTS) Putra World Trade Centre Kuala Lumpur, Malaysia (COMNETIT).
http://www.comnetit.org/strategies/criis2001/ma2001-w.pdf

Mongolia. (2002). Asia-Pacific Conference on Cybercrime and Information Security Seoul, Republic of Korea 11-13 November.

UNIT 2
Identity and Information Security Integration

Content

1.0 Introduction

In the past, identity management and information security solutions were often procured, implemented, and managed independently with different tools, processes, and organizational units. This separation is quickly becoming a thing of the past**.** Identity and security integration is already challenging technology vendors, not just IT professionals. There are various attempts addressing new user requirements by integrating their best-of-breed identity and security technologies in order to meet the changing needs of demanding enterprise customers.

2.0 Objectives

This unit examines the Historical Perspective of Identity and Security vis-à-vis the Need for Identity and Information Security Integration Students are therefore expected to know the concepts of Data discovery, classification, and security policy enforcement, Identity and Information Security Integration Requirements. These are clearly explained through ESG's organisational research.

3.0 Main body

Identity and Security: A Historical Perspective

Throughout the history of distributed computing, identity management and information security were often implemented and managed in a fairly independent fashion. Yes, security groups cooperated with software developers and IT operations on things like user authentication and password management, but overall collaboration remained fairly limited. For the most part, identity and security remained separate because:

Identity management focused on employee productivity. The process for provisioning a user account was generally led by the Human Resources Department as part of providing new employees with essential productivity tools like telephones, employee badges, and network/application access. While HR initiated the process, IT was responsible for many critical Identity and Access Management (IAM) tasks. Until fairly recently, many of these tasks were ad-hoc and manual, with IT administrators provisioning application and network accounts on a system-by-system basis. More recently, IT operations acquired more sophisticated identity management tools to automate user provisioning, workflow, and day-to-day operations, but these processes were still guided by HR and business managers.

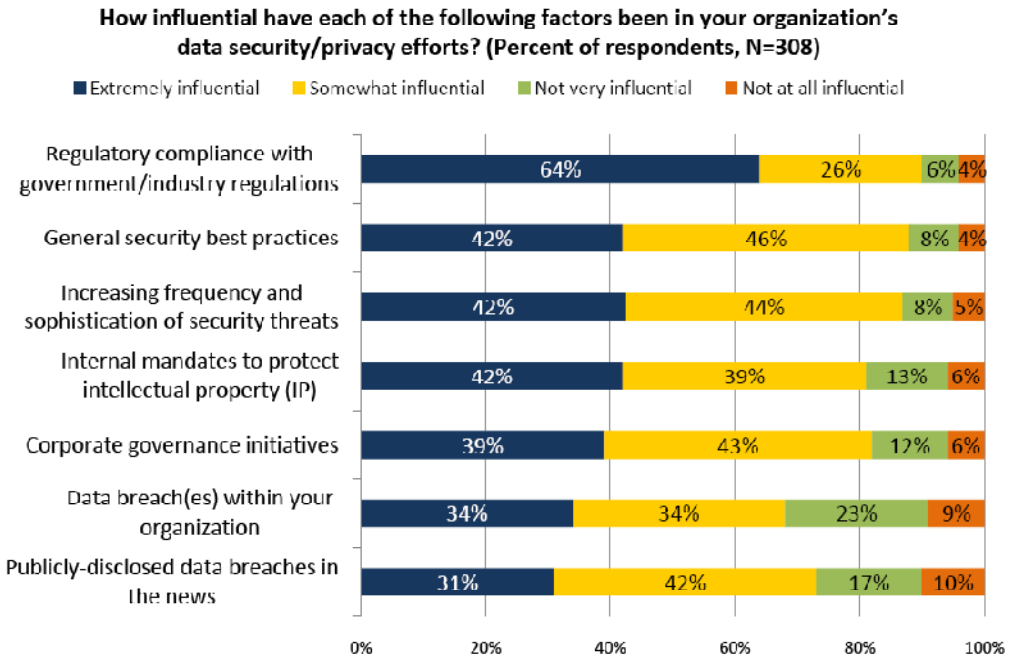
Security teams focused on IT infrastructure and security attacks. Far removed from HR, CSOs concentrated on safeguarding networks and PCs against hackers and malicious code. Security professionals were often highly focused on technologies like firewalls and antivirus software and were regarded as a niche group of specialists within IT. With the benefit of hindsight, it is hard to believe that security and identity operations were so far removed from one another, but this separation was logical at the time. Until recently, business computing was anchored by private networks and minimal Internet access, so "trusted" employees were thought of as a minimal security risk. Sure, a few rogue workers might steal office supplies, but this type of physical threat was all that was expected. Alternatively, IT security risks were pigeonholed into known attacks like the "I Love You" and "Melissa" e-mail viruses, web site defacement, and network scanning. Identity and security were binary topics – one dealt with trusted employees and the other with un-trusted network packets. These areas were distinct and disconnected within IT.

The Need for Identity and Information Security Integration

Fast forward to the last few years and there is growing IT consensus: identity and data-centric security technologies and processes must come together. Why? In 2009 and beyond, tight identity and data-centric security integration has become an enterprise requirement because:

Regulatory compliance requires strong access and security controls. Government and industry regulations such as Basel II, HIPAA, the EU Data Privacy Directive, and PCI DSS are forcing large organizations to implement security and identity policies and controls to restrict access to private/sensitive data (i.e., customer data, health care records, credit card numbers, etc.), log security events, and perform compliance audits on a regular basis. Since compliance violations can result in stiff penalties, costly data breaches, or even criminal charges, regulatory compliance (and associated identity and security integration) plays an extremely influential role in the data privacy/security efforts of large organizations (see Figure 1).

Figure 1. Influential Factors in Information Security/Privacy Efforts



Source: Enterprise Strategy Group, 2009.

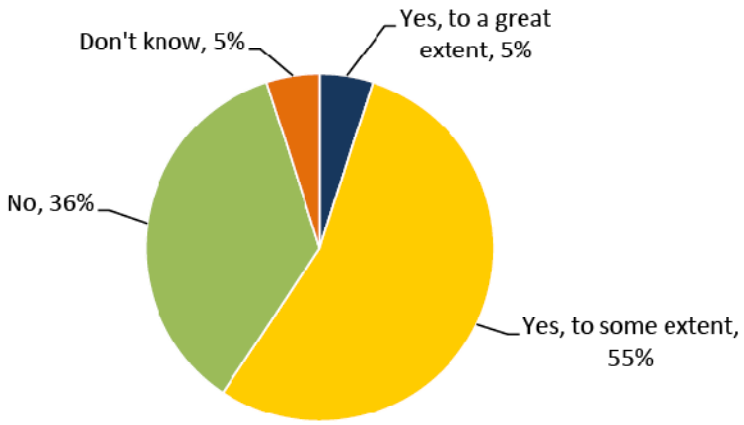
Costly data breaches are all too common occurrences. There were a total of 615 publicly-disclosed data breaches in 2008 exposing more than 83 million personal records (source: datalossdb.org). Approximately 21% of these incidents are the result of stolen or lost laptops, 17% are the results of "hacks," 14% are the results of attacks on web applications, and 7% are the result of fraud. To address the risk of a data breach in the future, CSOs need to control access to regulated private data, detect/prevent data leakage, and monitor user activity at all times.

Internal networks are "open for business." New business processes are often linked to web applications and Internet technologies in order to drive new revenue streams, expand opportunities, accelerate business initiatives, and lower costs. This trend is illustrated by ESG research data, where 60% of enterprise organizations (i.e. 1,000 employees or more) say that they share confidential data with non-employees (see Figure 2). Most organizations also believe that they will share more confidential data with more external constituencies like business partners, customers, or suppliers in the future as well. This trend means more and more users will live "outside the firewall." And with more and more business conducted over the network, large organizations can't simply block IP addresses, ports, and protocols. Alternatively, they need a clear understanding of who accessed sensitive data from which location. This demands tight identity/information security integration, constant user and network monitoring, and strong technologies for policy enforcement. Taken together, these factors break the old model of independent security and identity islands. Today's disparate identity and security infrastructure is anchored by multiple management platforms that can't provide for central control, end-

to-end monitoring, or common skills and processes. Protecting confidential data and meeting regulatory compliance requirements are dependent upon an army of IT administrators, manual processes, and costly fire drills. Even with this amount of effort, CSOs must piece the status of enterprise security together based upon disjointed data and personal opinions. In this scenario, enterprise information security is an educated guess at best. Since legacy tactical identity and security tools can't provide automation, command-and-control, or end-to-end oversight, CIOs find themselves at a technology crossroad: either proceed with identity and security integration or suffer the consequences of high costs, limited agility, and increased risk.

Figure 2. Most Large Organizations Share Confidential Data with Non-Employees

Does your organization share its confidential data with non-employees (i.e., business partners, suppliers, customers, etc.)? (Percent of respondents, N=308)



Source: Enterprise Strategy Group, 2009.

Think Identity and Access Assurance

Most identity management tools are designed for password management, application account provisioning, and role management. To meet today's new challenges, identity management must embrace information security knowledge in order to enforce access and entitlements at a more atomic level. With this intelligence, large organizations can then lock down data access to a small group of "need to know" users, monitor activity, and change access controls on the fly when necessary.

In order to achieve these goals, identity management needs to be integrated into a common "identity and access assurance" infrastructure with leading security safeguards like:

Data discovery, classification, and security policy enforcement.

The identity management infrastructure should be supported by Data Loss Prevention (DLP) tools that can scan and classify data repositories and endpoint systems for

sensitive data. Armed with this knowledge, identity and access management tools can be used to create small sub-groups or specific roles with confidential data access rights. In this way, information-centric identity management can help streamline regulatory compliance controls, simplify audits, and reduce information security risks.

Security monitoring and analysis.
Many existing compliance and security tools can only identify a user based upon an IP address, not by an actual account name. This is clearly inadequate as current and future compliance auditing and security forensic investigations demand an end-to-end review of who did what and when. To get a complete picture, identity auditing tools must align with log management and security event management data. This integration alone can greatly reduce the time and effort necessary for security event detection, root cause analysis, and emergency response.

Authentication management.
New demands for entitlements and role-based access controls demand a combination of automated account provisioning and strong authentication. When applied in an integrated fashion, account provisioning and authentication can make access rules far more granular to specific users, application functions, or data elements.

Access certification. In order to demonstrate compliance with industry and government mandates regarding controls over access to sensitive data, organizations need a mechanism for automatically analyzing user access rights and verifying that they are consistent with corporate policy.

It is important to note that identity and information security integration must go beyond information exchange for historical reporting. Today's business and security demand rapid response capabilities for functions like provisioning a user account for an external contractor, detecting a security attack in progress, or gathering evidence for a legal proceeding. To meet these requirements, identity and information security must have integrated command-and-control, common user interfaces, and real-time monitoring and alerting.

Identity and Information Security Integration Requirements
As described above, identity and information security integration is being driven by numerous business and technology trends. Moving forward, CIOs will need to be incredibly responsive to changing requirements with an identity and security infrastructure that can meet their requirements in 3 areas (see Table 1):
1. Real-time business agility
2. Ease of use.
3. Enhanced protection

Table 1. Attributes of Identity and Information Security Integration

Attribute	Business Benefit	IT Benefit
Real-time business agility	• Get users productive • Extend internal applications to external constituencies to drive revenue and productivity • Customize business processes to user needs and requirements	• Offer proactive support for new business processes • Accelerated deployment of new applications
Ease of use	• Rapid business process execution • Accelerates time to user productivity	• Rapid user provisioning • Rapid integration into IT infrastructure • Enhanced IT skills with common processes and training
Enhanced protection	• Secure business processes • Security seen as enabler, not an inhibitor	• Security from user access to back-end data • End-to-end enterprise coverage • Common view and reports for measurement, forensics, and compliance audits

Real-time Business Agility

First and foremost, an integrated identity and information security infrastructure must enable, rather than inhibit, new network-based business processes without increasing risk or complicating regulatory compliance efforts. To accomplish these goals, integrated identity and security must:

Get users productive—and keep them productive. Think of automated user account provisioning as "table stakes" here. Basic identity tools must tie into HR systems, anchor workflow processes, and handle moves/adds/changes in a straightforward fashion. Superior systems will also define and manage roles/entitlements, keep users productive with enterprise password management based upon corporate policies, and tie into user access compliance tools that review access rights, detect control gaps, and guide IT administrators through remediation processes. The best identity tools will also interoperate with existing directory infrastructures rather than require a costly and complex directory overlay. Ultimately, the goal is to maintain productivity by making tasks like application authentication, password management, and management approval processes as automated and transparent as possible.

Accommodate non-employees. As ESG's research clearly indicates, moving forward, more and more users will be external constituents rather than employees. While external IT applications help the business, IT may be quickly overwhelmed if it is expected to provision external users via internal tools and processes. To align external business processes with IAM requirements, it is imperative that CIOs set up the right processes and technologies to accommodate federated identity. With the appropriate tools and

support for federated standards, an integrated identity/security infrastructure can extend security, authentication, authorization, and user account provisioning to business partners and vice versa. When supported by the right contractual protection and IT/end-user training, federated identity can greatly accelerate external business initiatives without adding operations overhead or incremental risk.

Align access rights with business processes. While most large organizations have standard security policies, IT utilization and risk tolerance varies greatly on a business process basis. For example, a health care facility will customize access rights and security policies depending upon whether business processes centre around urgent care, prescription management, or administration. By marrying identity and information security, large organizations can create authentication and authorization policies based upon additional factors such as location, time of day, and type of transaction. When a physician accesses patient records from the emergency room, she will be given immediate access based upon her RFI identity badge. When she prescribes painkillers for this patient, she may be asked for additional access verification before the transaction can be processed.

Ease of Use

Even in the most sophisticated IT shops, many business and IT managers would agree that current identity and security processes and tools are overly complex and cumbersome. Today's annoyances could quickly cascade into major impediments as the number of external users and network business processes skyrocket. Clearly, this must change quickly. To support growing business needs, identity and security integration "ease of use" must be drastically improved with: Integrated command-and-control. Today's patchwork identity and security infrastructure is anchored by a potpourri of management and reporting consoles that can't scale, coordinate change management, or offer common reporting. While a single management platform would be ideal, the reality in today's diverse, heterogeneous environment is that vendors must integrate disparate tools and technologies. In the short term, identity and security must be backed by integrated management tools that share information while coordinating configuration and change management operations. With identity and security integration, a security or compliance manager can evaluate user access rights or roles as they relate to sensitive data, like health information, in a common report. By viewing this data in a common report, they can easily take the necessary remediation actions like verifying access privileges with a business manager, adjusting policies, or modifying user access rights accordingly.

Wide support for applications and devices.

The history of IAM is plagued by limited software tools that demand complex and time consuming custom integration. CIOs should no longer put up with this burden. Rather, IAM systems designed for today's business requirement must provide "out-of-the-box" support for a wide assortment of business applications, security technologies, and

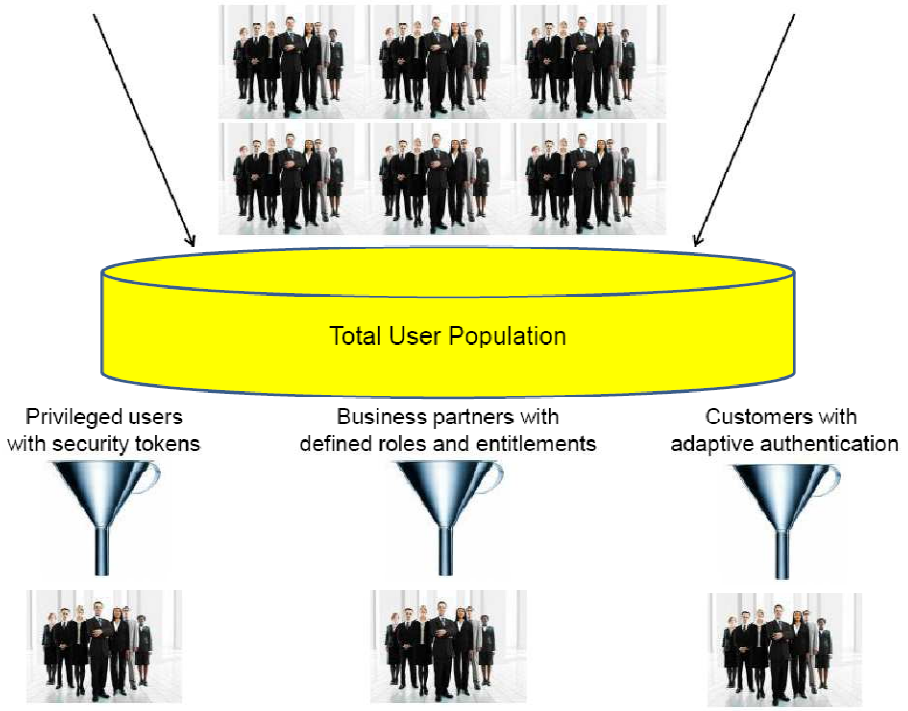
hardware devices. For example, IAM tools should seamlessly plug into hard and soft authentication technologies for user provisioning as well as configuration and change management. Account and role management systems should work flawlessly with web access management systems that often control access to external applications. Internal systems should also support federated identity standards to simplify integration with external users and applications. User self service. Regardless of training efforts, many users will still need help with new identity tools, lose their security tokens, or forget their passwords. This usually ends with a help desk call carrying an associated cost. Yes, it is important to provide adequate services for end-users, but user self service tools have demonstrated their value in accelerating problem solving and greatly reducing help desk call volume. The best identity tools provide an assortment of self service capabilities, such as password reset or business manager-based user provisioning. All of these capabilities bolster productivity while minimizing IT involvement.

Enhanced Protection

Of course, the other side of accelerated business processes is risk management. More users, devices, network traffic, and web-facing applications have the potential to greatly increase security risk. To address these threats while supporting the business, identity and security integration must:

Support strong authentication and fine-grained access control. To deal with issues around identity theft, users accessing sensitive or private data should use some type of authentication technology that offers greater security than a typical user name and password. Aside from standard account provisioning, this requires account management systems capable of provisioning one-time passwords or risk-based authentication technologies such as adaptive authentication (i.e., challenge/response systems), as well as application access-based rules based upon organizational risk posed by users, groups, or specific roles. This functionality creates a “funnel effect” in order to segment the total population of users into more discrete, manageable, and secure sub-groups (see Figure 3).

Figure 3. Identity and Security Used to Segment Total User Population into Manageable Sub-groups



Source: Enterprise Strategy Group, 2009.

Augment information security controls. Entitlement management success depends upon data discovery, classification, and rights management. This is best accomplished with an integrated identity and security infrastructure that includes DLP in the data centre, in the network, and on endpoints. In this scenario, DLP is used to scan and classify data repositories and apply data access rules that align with roles and security policies. In the best case, identity tools can support DLP by mapping confidential data files directly with user access rights. This helps apply a sense of context to access policies by mapping data classification with user roles. In this way, security administrators can ensure that only authorized personnel have access to sensitive data. When Margaret in HR tries to download the employee database, security administrators can quickly determine her identity and location and then take remediation actions to cut off her network access and cancel her account. Provide end-to-end monitoring and reporting. Governance, risk, and compliance efforts depend upon a steady stream of real-time information to assess current status, detect anomalies or attacks, analyze events, and compile reports for management reviews or IT audits. Integrating identity and security with Security Information and Event Management (SIEM) can enhance current monitoring and reporting tools by linking security events to actual people and transactions. When Eddie in Sales suspects that he will be terminated soon and begins stealing customer information, security administrators will be able to link large file downloads to Eddie himself, rather than to a

cryptic IP address. This capability is also extremely useful for security event detection and investigation. Managers can also use access certification and compliance management software to examine and validate that user access rights to sensitive data are consistent with the "least privilege" principle and that access is based on a clearly defined business purpose.

Taken together, these identity and security integration attributes can help CIOs achieve their biggest objectives: provide technology tools to accelerate the business while minimizing any incremental risks. Aside from these worthwhile goals, large organizations can experience some other significant benefits as well. First, they will be able to customize business processes and security policies based upon user or group attributes. For example, IT can create application features and provide secure access for only a handful of top customers to increase sales and customer satisfaction. This can lead to more creative and experimental applications. Finally, IT can greatly reduce the costs associated with IAM and security through greater use of automation, user self-services, and common management/reporting Since users managed identity and security separately in the past, many technology vendors picked their battles in one area or another, so there are few integrated solutions to choose from. The story is actually worse than this, however. Many "integrated" identity and security solutions were either cobbled together through acquisition or depend upon basic interoperability between various vendor offerings.

Self Assessment Exercise

Explain the Need for Identity and Information Security Integration

4.0 Conclusion

Along with death and taxes, integration of identity and security is inevitable. CIOs must recognize this reality soon and address the current gaps between the two areas. While IT operations, compliance, and security groups will benefit from an integrated identity and security infrastructure, smart IT executives will make sure to work hand-in-hand on this transition with business managers as well. Use this as an opportunity for IT and the business to collaborate on things like data classification, user roles, self-service requirements, and workflow process improvements. Smart CIOs will assess their current identity and information security tools and begin crafting a migration plan toward integrated identity and access assurance. To avoid past mistakes and move forward on a proactive basis, IT executives should:

Gain buy-in from the business. As mentioned above, CIOs should use this project as an opportunity to get business managers involved. This means defining policies, data classification taxonomies, roles, and workflows and then aligning monitoring and enforcement technologies with clearly defined business processes. Make sure to define

"ease of use" requirements as well, in order to deliver an identity and access assurance infrastructure that business managers will support.

Appoint and empower project managers. Even if business and IT requirements are clearly defined, things will change as identity/security projects progress. Make sure that project managers have enough internal clout to manage through these changes. Savvy organizations will support project managers with business and IT executive oversight.

Require a proof of concept. Make sure that identity and access assurance projects contain a proof-of-concept phase so project managers gain experience from a final test on functionality and usability by a broad group of business, IT, and security managers.

Look for "out-of-box" capabilities. Even the best project can be detoured by months of custom software design, development, and testing. To avoid these interruptions, make sure to select tools that offer the broadest "out-of-box" support for application/device support, policy creation, custom reports, and information security integration. Vendors and reference accounts that provide nebulous information about multi-year implementation cycles, development tools, or vague information security partnerships should be viewed as a red flag.

Finally, software and services acquisition costs are important, but the real goal should be long-term TCO, risk reduction, and business enablement. Make sure to ask reference accounts for concrete data on how they've done in these areas.

5.0 Summary

This unit highlights the importance of identity management, identity and security integration attributes for any organisational structure and for management staff. Mentioned among others are the attributes which can help major players in large organisations to achieve their objectives, in providing relevant technological tools to accelerate the business process while minimizing any incremental risks.

6.0 Tutor Marked Assignment

a. What is Identity management?
b. Why has overall collaboration between security groups, software developers, and IT operations remained fairly limited?

7.0 References/ Further Reading

Baskerville R & Wood-Harper T (1996) A Critical Perspective on Action Research as a Method for Information Systems Research. Journal of Information Technology 11: 235-246.

Chaiken S (1980) Heuristic versus systematic information processing and the use of source versus message cues in persuasion. Journal of Personality and Social Psychology 39: 752-766.

Denning DE (1999) Information Warfare and Security. ACM Press, USA.

Desman MB (2002) Building an IS security Awareness Program. Auerbach Publications, USA.

Hadland T (1998) IS security management - an awareness campaign. Proceedings of New Networks, Old Information: UKOLUG98, UKOLUG's 20th Birthday Conference 1998.

Hansche S (2001) Designing a Security Awareness Program: Part I, Information system security 10(1): 14-22.

Kovacich GL (1998) Information system security Officer's Guide: Establishing and Managing an Information Protection Program. Butterworth-Heinemann, USA.

UNIT 3

Integrating Information Assurance into System Administration

Content

1.0 Introduction

The ability to construct virtual information systems either locally or using a wide range of options from externalizing individual services to a fully distributed or cloud computing environment rapidly implies that system administrators may not only be called upon much more frequently to make decisions that would previously have been the prerogative of system architects, but that such decisions may be based more on momentary expediency than sound architecture as it may be faster and more cost-effective to call upon an external service provider than to bring internal services on-stream. Moreover, the use of services rather than capital equipment and the prospect of off-loading most of the administrative responsibility associated with such services all provide strong incentives at levels from system administrators to system architects. The use of such facilities does, however, involve a number of risks both technical and legal in nature which must be fully understood as some of the consequences of service use are difficult if not impossible to reverse and hence can have a temporal extent that far exceeds the life-time of a given configuration. At the same time it is unlikely that, as requirements emerge at the operational level, decisions on how to meet requirements will be escalated to a strategic system architect's level at all time. Given that many such services are, however, interdependent on each other either directly or indirectly, even a small number of externally provisioned services can represent a long-term commitment.

2.0 Objectives

Based on the above introduction students are expected to understand:

1. The types of services and facilities available to information system architects and administrators.
2. Information security implications.

3.0 Main body

Distributed computing services, despite recent and periodic re-naming and different efforts at promoting such services, has been a long-standing vision arguably originating with the *Computing Utility* proposed by the MIT MAC project as articulated by Fano (1965) and subsequently implemented substantially in the Multics system. It is particularly noteworthy in this context that one of the core concepts of modern cloud computing, i.e. the sharing and remote commercial use of virtual machines dates to the mid- 1960s.

Key Features Of Current Distributed Computing Architectures

While terminology varies considerably, a simple taxonomy of distributed computing elements can be derived based on the granularity of the services offered. At the finest level of granularity, individual services, typically web or database services (currently being referred to as *applications in the cloud* or AITC) are providing business processes or components with state distributed across servers and client systems. Several implementation variants, frequently hybrid, ranging from legacy CORBA environments via SOAP and WS infrastructures to AJAX based on the design principle of representational state transfer (REST) originally articulated by Fielding (2000). Each service may in turn depend on others and can require several service layers (frequently employing database back-ends). Moreover, a number of ancillary services can be required, including service discovery mechanisms, name services and, when security mechanisms are utilized, key management infrastructures. Moreover, each of these services can be provided in a geographically distributed manner, adding the interconnecting networks to the infrastructure required for provisioning such services. While general deployment of such services is limited, some areas such as externally provisioned email services are increasingly common.

Similar design principles employing middleware components are also found in more complex service-oriented architectures in which complex business processes are composed of multiple implementation services and events typically coordinated on enterprise service bus responsible for process choreography and service orchestration; this is also referred to as *platforms in the cloud* (PITC). Software as a service (SaaS) as originally described by Bennett *et al.* (2000) can be considered a derivative of this approach in that the service delivery uses the same technical underpinnings while state is typically retained on the application service provider's systems; infrastructure dependencies are therefore potentially of similar complexity as in the case of uncoupled web services. However, the most popular approach commonly associated with the term cloud computing (also referred to as *infrastructure in the cloud*, IITC) is of a more coarse granularity in that it is centred on the provisioning of virtual machines and storage space available commercially from a number of sources. Although this eliminates some of the interdependency layers noted above, access to services will still require queuing, network and cryptographic key management as well as potentially front-end infrastructures, while

both virtual machines and storage will frequently be re-located dynamically to provide improved response times and failure tolerance as well as load balancing.

Cloud Management

Although particularly in case of IITC residual system management responsibility lies with the service user and network as well as enabling infrastructure must still be maintained, significant portions are migrating to the infrastructure provider. This requires not only the elaboration of service level agreements (SLA) for all relevant aspects of the service, but also monitoring compliance with SLAs and the deployment of mitigation and service level enforcement mechanisms.

SECURITY CHALLENGES

A number of security issues arising from the distributed environments outlined in section 2 are easily identified. While securing confidentiality and integrity of data in transit is trivially addressed using standard cryptographic protocols, even storage presents a number of difficulties as encrypting data at rest may both interfere with desired functionality and adversely affects application performance. Moreover, as data is processed, by definition, on systems under the control of one or more third parties, it will be available as plaintext in such an environment. This raises questions both about the trustworthiness of service providers and the strength of compartmentalization between virtual machine instances, which must not only be maintained during operation but also in case of virtual machine migration.

Further security issues arise from uncertainties about the integrity of the computing and communication platform themselves, which can affect the integrity of both the applications and that of active monitoring, e.g. by Byzantine behaviour in suppressing or altering messages. This type of threat is also present for the case of key and identity management; as key material is implicitly exposed, it may be accessible to adversaries at endpoints or within the management infrastructure of the service provider. Given the exposure of network traffic as well as potential cross-service contamination and hence the increased risk of denial of service attacks compared to systems within an organization’s perimeter, availability is a major security consideration. While reliability models can provide predictable high levels of availability in the face of random (Gaussian) failures, this may not be the case for deliberate attacks, which may indeed target the very mechanisms providing robustness and redundancy such as load balancing mechanisms. However, while the above touches upon several critical and in part insufficiently resolved security challenges in cloud computing, there are further implications for legal and management perspectives which must also be taken into account.

In most backup configurations, multiple copies and generations of backup data are interspersed on storage media at different access hierarchies. While this redundancy is typically desirable in the event of failure, deletion of data sets such as in case of the termination of a service agreement is problematic, particularly if a service provider does

not isolate backups for different customers as is commonly the case and implied in terms and conditions of service providers. Similarly, both servers and storage media may be in different physical locations with services and data migrating among locations to provide optimum resource usage and service levels. However, while such migration and distribution is deliberately transparent at the implementation level, physical location can imply that a given datum or service may fall under different jurisdiction. In some cases this may even affect the legality of a service or transactions, but a major concern arises from the possibility of seizing evidence in criminal or civil proceedings as well as for compliance purposes. Moreover, certain processes may rule out the use of cloud computing environments entirely.

Self Assessment Exercise

1. What is cloud computing?
2. Discuss some of the security challenges.

4.0 Conclusion

While the cost and flexibility benefits resulting from distributed and cloud computing environments are clearly evident, this approach also has far reaching implications for the threat surface presented as well as general information security risks, particularly to availability. The design of cloud-based storage services also implies that data once stored with such services may be very hard to recall. The ease with which these services can be used implies that system administrators may not only be called upon much more frequently to make decisions that would previously have been the prerogative of system architects, but that such decisions may be based more on momentary expediency than sound architecture unless the implications are understood clearly. As the impact is both technical and legal in nature and can easily have a temporal extent well exceeding the life-time of a given configuration.

5.0 Summary

This unit briefly reviews some of the key features of current distributed computing architectures; it highlights systems management aspects of such architectures.

6.0 Tutor Marked Assignment

Residual system management responsibility has been described as lying with the service user and network as well as enabling infrastructure. Discuss.

7.0 References/ Further Reading

Bennett, K. P. Layzell, D. Budgen, P. Brereton, L. Macaulay, and M. Munro. Service-based software: the future for flexible software. In *Proceedings of the Seventh Asia-*

Pacific Software Engineering Conference (APSEC 2000), pages 214–221, Singapore, December 2000. IEEE Press.

Corbato F. J. and V. A. Vyssotsky. Introduction and Overview of the Multics System. In *Proceedings of the AFIPS Fall Joint Computer Conference (1965 FJCC)*, volume 27 part 1, pages 185–196, Las Vegas, NV, USA, November 1965. AFIPS, Spartan Books.

Fan, M. Kumar, S. and Whinston,. A. B. (2009). Short-term and long-term competition between providers of shrink-wrap software and software as a service. *European Journal of Operational Research*, 196(2):661–671, July

Fano. R. M. (1965). The MAC System: The Computer Utility Approach. *IEEE Spectrum*, 2(1):55–64, January 1965.

Fielding, (2000). R. T. *Architectural Styles and the Design of Network-based Software Architectures*. PhD thesis, Department of Information and Computer Science, University of California, Irvine, Irvine, CA, USA,

UNIT 4

Management Information Systems Usability and Associated Risk

Content

1.0 Introduction

A management information system (MIS) is a system or process that provides the information necessary to manage an organization effectively. MIS and the information it generates are generally considered essential components of prudent and reasonable business decisions. The importance of maintaining a consistent approach to the development, use, and review of MIS systems within any institution must be an ongoing concern for management and technical staff.

.

2.0 Objectives

Students are expected to know:

1. the basic definition of Management Information Systems
2. the relevance of management information system (MIS) and how it should be designed and used to achieve sound organisational goals.
3. the various risks associated with the management of MIS.

3.0 Main body

MIS should have a clearly defined framework of guidelines, policies or practices, standards, and procedures for the organization. These should be followed throughout the institution in the development, maintenance, and use of all MIS. MIS is viewed and used at many levels by management. It should be supportive of the institution's longer term strategic goals and objectives. To the other extreme it is also those everyday financial accounting systems that are used to ensure basic control is maintained over financial record-keeping activities. For instance Financial accounting systems and subsystems are just one type of institutional MIS. Financial accounting systems are an important functional element or part of the total MIS structure of a bank. However, they are more narrowly focused on the internal balancing of an institution's books to the general ledger and other financial accounting subsystems. For example, accrual adjustments, reconciling and correcting entries used to reconcile the financial systems to the general ledger are not always immediately entered into other MIS systems. Accordingly, although MIS and accounting reconcilement totals for related listings and activities should be similar, they may not necessarily balance.

An institution's MIS should be designed to achieve the following goals:

- Enhance communication among employees.
- Deliver complex material throughout the institution.
- Provide an objective system for recording and aggregating information
- Reduce expenses related to labour-intensive manual activities.
- Support the organization's strategic goals and direction.

Because MIS supplies decision makers with facts, it supports and enhances the overall decision making process. MIS also enhances job performance throughout an institution. At the most senior levels, it provides the data and information to help the board and management make strategic decisions. At other levels, MIS provides the means through which the institution's activities are monitored and information is distributed to management, employees, and customers. Effective MIS should ensure the appropriate presentation formats and time frames required by operations and senior management are met. MIS can be maintained and developed by either manual or automated systems or a combination of both. It should always be sufficient to meet an institution's unique business goals and objectives. The effective deliveries of an institution's products and services are supported by the MIS. These systems should be accessible and useable at all

appropriate levels of the organization. MIS is a critical component of the institution's overall risk management strategy. MIS supports management's ability to perform such reviews. MIS should be used to recognize, monitor, measure, limit, and manage risks. Risk management involves four main elements:

a) Policies or practices.
b) Operational processes.
c) Staff and management.
d) Feedback devices.

Frequently, operational processes and feedback devices are intertwined and cannot easily be viewed separately. The most efficient and useable MIS should be both operational and informational. As such, management can use MIS to measure performance, manage resources, and help an institution comply with regulatory requirements. One example of this would be the managing and reporting of loans to insiders. MIS can also be used by management to provide feedback on the effectiveness of risk controls. Controls are developed to support the proper management of risk through the institution's policies or practices, operational processes, and the assignment of duties and responsibilities to staff and managers.

Technological, advances have increased both the availability and volume of information management that directors have for both planning and decision making. Correspondingly, technology also increases the potential for inaccurate reporting and flawed decision making. Because data can be extracted from many financial and transaction systems, appropriate control procedures must be set up to ensure that information is correct and relevant. In addition, since MIS often originates from multiple equipment platforms including mainframes, minicomputers, and microcomputers, controls must ensure that systems on smaller computers have processing controls that are as well defined and as effective as those commonly found on the traditionally larger mainframe systems. All institutions must set up a framework of sound fundamental principles that identify risk, establish controls, and provide for effective MIS review and monitoring systems throughout the organization. Commonly, an organization may choose to establish and express these sound principles in writing.

Placing these principles in writing is often the best option to enhance effective communications throughout any institution. If however, management follows sound fundamental principles and governs the risk in the MIS, a written policy will not be required. If sound principles are not effectively practiced, the organisation may require management to establish written MIS policies to formally communicate risk parameters and controls in this area. Sound fundamental principles for MIS include proper internal controls, operating procedures and safeguards, and audit coverage. These principles are explained below.

Risks Associated With Management Information Systems

Risk reflects the potential, the likelihood, or the expectation of events that could adversely affect earnings or capital. Management uses MIS to help in the assessment of risk within an institution. Management decisions based upon ineffective, inaccurate, or incomplete MIS may increase risk in a number of areas such as credit quality, liquidity, market/pricing, interest rate, or foreign currency. A flawed MIS causes operational risks and can adversely affect an organization's monitoring of its fiduciary, consumer, fair lending, Bank Secrecy Act, or other compliance-related activities. Since management requires information to assess and monitor performance at all levels of the organization, MIS risk can extend to all levels of the operations. Additionally, poorly programmed or non-secure systems in which data can be manipulated and/or systems requiring ongoing repairs can easily disrupt routine work flow and can lead to incorrect decisions or impaired planning.

Assessing Vulnerability To Management Information Systems Risk

To function effectively as an interacting, interrelated, and interdependent feedback tool for management and staff, MIS must be "useable." The five elements of a useable MIS system are: timeliness, accuracy, consistency, completeness, and relevance. The usefulness of MIS is hindered whenever one or more of these elements are compromised.

1. Timeliness

To simplify prompt decision making, an institution's MIS should be capable of providing and distributing *current* information to appropriate users. Information systems should be designed to expedite reporting of information. The system should be able to quickly collect and edit data, summarize results, and be able to adjust and correct errors promptly.

2. Accuracy

A sound system of automated and manual internal controls must exist throughout all information systems processing activities. Information should receive appropriate editing, balancing, and internal control checks. A comprehensive internal and external audit program should be employed to ensure the adequacy of internal controls.

3. Consistency

To be reliable, data should be processed and compiled consistently and uniformly. Variations in how data is collected and reported can distort information and trend analysis. In addition, because data collection and reporting processes will change over time, management must establish sound procedures to allow for systems changes. These procedures should be well defined and documented, clearly communicated to appropriate employees, and should include an effective monitoring system.

4. Completeness

Decision makers need complete and pertinent information in a summarized form. Reports should be designed to eliminate clutter and voluminous detail, thereby avoiding "information overload."

5. Relevance

Information provided to management must be relevant. Information that is inappropriate, unnecessary, or too detailed for effective decision making has no value. MIS must be appropriate to support the management level using it. The relevance and level of detail provided through MIS systems directly correlate to what is needed by the board of directors, executive management, departmental or area mid-level managers, etc. in the performance of their jobs.

Achieving Sound Management Information Systems

The development of sound MIS is the result of the development and enforcement of a culture of system ownership. An "owner" is a system user who knows current customer and constituent needs and also has budget authority to fund new projects. Building "ownership" promotes pride in institution processes and helps ensure accountability. Although MIS does not necessarily reduce expenses, the development of meaningful systems, and their proper use, will lessen the probability that erroneous decisions will be made because of inaccurate or untimely information. Erroneous decisions invariably misallocate and/or waste resources. This may result in an adverse impact on earnings and/or capital. MIS which meets the five elements of useability is a critical ingredient to an institution's short- and long-range planning efforts. To achieve sound MIS, the organization's planning process should include consideration of MIS needs at both the tactical and strategic levels. For example, at a tactical level MIS systems and report output should support the annual operating plan and budgetary processes. They should also be used in support of the long term strategic MIS and business planning initiatives. Without the development of an effective MIS, it is more difficult for management to measure and monitor the success of new initiatives and the progress of ongoing projects. Two common examples of this would be the management of mergers and acquisitions or the continuing development and the introduction of new products and services.

Management needs to ensure that MIS systems are developed according to a sound methodology that encompasses the following phases:

- Appropriate analysis of system alternatives, approval points as the system is developed or acquired, and task organization.
- Program development and negotiation of contracts with equipment and software vendors.
- Development of user instructions, training, and testing of the system.
- Installation and maintenance of the system.

Management should also consider use of "project management techniques" to monitor progress as the MIS system is being developed. Internal controls must be woven into the processes and periodically reviewed by auditors. Management also should ensure that managers and staff receive initial and ongoing training in MIS. In addition, user manuals should be available and provide the following information:

- A brief description of the application or system.
- Input instructions, including collection points and times to send updated information.
- Balancing and reconciliation procedures.
- A complete listing of output reports, including samples.

Depending on the size and complexity of its MIS system, an institution may need to use different manuals for different users such as first-level users, unit managers, and programmers.

Self Assessment Exercise

Discuss the four major elements involve in risk management.

4.0 Conclusion

The importance of Management Information Systems (MIS) to modern day institutions cannot be overemphasised if one is to weigh the benefits in the short and long run. Similarly the rate at which information flows in any organisation as well as the minimisation of risk in modern day businesses cannot be measured. It therefore calls for its implementation in any 21st century organisation properly called.

5.0 Summary

This unit examines the definition and relevance of Management Information System (MIS) and how it should be designed and used to achieve sound organisational goals. Much Emphasis was placed on the five elements of a useable MIS system which are: timeliness, accuracy, consistency, completeness, and relevance. In the same vein it highlights various risks associated with the management of MIS. Lastly the unit concluded with the relevance of MIS in any 21st century organisation.

6.0 Tutor Marked Assignment

List and explain the goals of any institution's Management Information Systems.

7.0 References/Further Reading

COBIT Security Baseline. USA: IT Governance Institute; 2004. www.itgi.org.

Comptroller’s Handbook. 1995. Management Information Systems. A Call to Actionfor Corporate Governance. IIA, AICPA, ISACA,NACD, www.theiia.org/eSAC/pdf/BLG0331.pdf; March 2000.

IBM offers companies monthly security report, www.nwfusion. com/news/2004/1025bmoffer.html.

Information Security Governance e a call to action, National Cyber Security Summit Task Force, www.cyberpartnership. org/InfoSecGov4_04.pdf.

Information Security Governance: guidance for Boards of Directors and Executive Management, IT Governance Institute, USA. ISBN 1-893209-28-8, www.itgovernance.org.

ITWeb. South Africa; 16 May 2003 Sarbanes-Oxley Act, www.sarbanes-oxley-forum.com.

UNIT 5

Elevating Information Security to Business Security

Content

1.0 Introduction

During the last year or two, driven by developments in the field of Corporate Governance, including IT Governance, it became apparent that the scope of Information Security is much wider than just (directly) protecting the data, information and software of a business. Such data, information and software had become invaluable assets of the business as a whole, and not properly protecting this information could have profound business and legal implications. Basically, the data and information of the business became its 'life blood', and compromising this life blood, could kill the business.

2.0 Objectives

Students are expected to know that the discipline responsible for protecting a company's information assets against business risks has now become such a crucial component of good Corporate Governance.

3.0 Main body

Executive Management and Boards started realizing that Information Security Governance was becoming their direct responsibility, and that serious personal consequences, specifically legally, could flow from ignoring information security. Information security governance had become an important business responsibility, and accountability escalated up to the Board level.
The following views quoted from relevant documents illustrate this development:

> 'Corporate Governance consists of the set of policies and internal controls by which organizations, irrespective of size or form, are directed and managed. Information security governance is a subset of organizations' overall (corporate) governance program' (Information Security Governancee a call to action).

> ‘Boards of Directors will increasingly be expected to make information security an intrinsic part of governance, preferably integrated with the processes they have in place to govern IT’ (Information Security Governance: guidance for Boards of Directors and Executive Management).
>
> ‘For information security to be properly addressed, greater involvement of boards of directors, executive management and business process owners is required’ (Information Security Governance: guidance for Boards of Directors and Executive Management).
>
> ‘An information security program is a risk mitigation method like other control and governance actions and should therefore clearly fit into overall enterprise governance’ (Information Security Governance: guidance for Boards of Directors and Executive Management).
>
> ‘The information possessed by an organization is among its most valuable assets and is critical to its success. The Board of Directors, which is ultimately accountable for the organization’s success, is therefore responsible for the protection of its information. The protection of this information can be achieved only through effective management and assured only through effective board oversight’ (A Call to Action for Corporate Governance, 2000).

One of the risks Board members are exposed to is:

> ‘Failure to understand the impact of security failures on the business, and potential effect on shareholders, share price and competition’ (COBIT Security Baseline, 2004).

This growing realization has established the fact that information security governance has an enterprise wide risk mitigating impact, and that the risks mitigated by an information security governance plan, are risks which have an enterprise wide business implication. After all, we do not refer to such risks as ‘information risks’, but to ‘business risks’, accepting and understanding the fact that if such risks materialize, business as a whole will be affected. Therefore, if we accept that such protection mitigates business risks, should we not start calling it Business Security instead of Information Security?

By ‘elevating’ Information Security to Business Security, it will get the extra focus and attention it needs to ensure the prolonged existence of the company, and to integrate all the present efforts as far as such protection is concerned. IBM has its Global Business Security Index, which is ‘aimed at the boardroom rather than IT departments because it

helps companies assess their security vulnerabilities from a business perspective.' (IBM). Note that they do not call it an 'Information Security Index', but rather a 'Business Security Index'!

Information Security Governance has become integral to good corporate governance. Although this fact had always been true (by default), this recent emphasis on good corporate governance had brought information security much more 'into the open', and 'into the faces' of Boards of Directors and Executive Management. This move had resulted in information security actually being seen as what it always was, a discipline to mediate business risks. This has also now been formulated in law by for e.g. the Sarbanes-Oxley legal developments in the USA. This development will however have an impact much wider than the USA. Other legal implications are also becoming apparent. 'Finally, company directors should keep in mind that failure and/or refusal to identify and address corporate IT risk may result in personal liability if damages or losses follow.

In terms of section 424 of the Companies Act, a director and even an IT manager may be personally liable for unlimited damages if the failure to identify and manage risks are classified as reckless management of the company by the courts' (ITWeb, 2003). Data security became computer security, and computer security became IT security and IT security became information security because of the better understanding of the business impact and associated risk of not properly protecting a company's electronic resources. The recent emphasis and guidelines on good corporate governance had improved and extended this understanding to such an extent that this protection must now be seen as an integral part of wider business protection and Business Security seems to be the best term to relate the fact.

Self Assessment Exercise

What do you understand by Information security governance?

4.0 Conclusion

There are various views regarding the term Business Security as too wide to use in this context - nevertheless, it is important that by starting to refer to Information Security as Business Security, and Information Security Governance as Business Security Governance, the role and position of protecting the electronic resources of a company will just benefit by making it a permanent item within the protection of the business as a whole, and of mediating business risks - as is required by good Corporate Governance.

5.0 Summary

This unit argues that information security, the discipline responsible for protecting a company's information assets against business risks, has now become such a crucial component of good Corporate Governance, that it should rather be elevated from Information Security to Business Security or better still be used interchangeably.

6.0 Tutor Marked Assignment

1. What are the benefits of elevating Information Security to Business Security?
2. Succinctly define Corporate Governance and list its components?

7.0 References/Further Reading

Barwise, J and Etchemendy J. (2001). "Computers, Visualization, and the Nature of Reasoning." Accessible in PDF format via *http://morpheus.hartford.edu/~anderson/*

COBIT Security Baseline. USA: IT Governance Institute; 2004. www.itgi.org.

IBM offers companies monthly security report, www.nwfusion. com/news/2004/1025bmoffer.html.

Information Security Governance e a call to action, National Cyber Security Summit Task Force, www.cyberpartnership. org/InfoSecGov4_04.pdf.

Information Security Governance: guidance for Boards of Directors and Executive Management, IT Governance Institute, USA. ISBN 1-893209-28-8, www.itgovernance.org.

Information Technology Web. (2003). South Africa; 16 May, Sarbanes-Oxley Act, www.sarbanes-oxley-forum.com.

Kendell, K.E. and Kendell, J.E. (2002). Systems Analysis and Design. Pearson Education Asia Pp.117-196.

Module 3

Unit 1. The Information Systems and the Economics of Innocent Fraud Management
Unit 2. An Overview of Information Security as a Risk Management Function
Unit 3. Risk Assessment
Unit 4. Risk Mitigation Options
Unit 5. Mitigating Economic Risk through Security Technology

Unit 1
The Information Systems and the Economics of Innocent Fraud Management
Contents

1.0 Introduction

In a published work, a concise and illustrated synthesis of what may be considered indeed an intellectual will, John Kenneth Galbraith defines the present economic system as 'the economics of innocent fraud' (Galbraith, 2004). This is an economy estranged from the real world, an economy where the private sphere directs the public one (through the defense and arms industry) and where corporations work antidemocratically (the power is

in the hands of those who own a minority of shares). This is also an economy in which the poor are denied access to the money they need to spend whereas the rich are granted the income they will save (according to Galbraith, this is the main effect of the tax cuts policies worldwide). And this is also an economy in which an elite of great men pretend to know what is not possible to know, the uncertainties of economic change (charging huge fees for it). In short, this is an economy which constitutes a real fraud to mankind. This fraud could be more or less 'innocent': it is sometimes an uncalculated status, taken for granted and assimilated by the majority as normal, and perpetuated with good intentions, starting by the mass media which do not condemn it; whereas at other occasions it carries an implicit and considerable burden of selfishness and malice.

2.0 Objectives

Students are expected to describe the connection between the use of ICTs and financial crime; and the need for ICTs as a tool to fight the lack of transparency and white-collar crime.

3.0 Main body

Information and Communication Technologies and its Democratizing Role

According to the World Bank, the ICT sector is defined as the sum of hardware, software, and networks subsectors plus the media for retrieving, storing, processing, transmitting and presenting information (voice, data, text, images) (World Bank Group, 2002). The ICT sector has involved a whole revolution throughout the most diverse areas of society, as has been recurrently and prolifically described previously, by a considerable number of authors during the last two decades (for example Castells, 1997; Shapiro and Leone, 1999; Lessig, 1999; Slevin 2000; or Himanen, 2001). Nevertheless, some productive sectors have been especially affected by the idiosyncrasy of the change; amongst them are the financial sector and the mass media. Firstly, in the case of the financial services , we are facing the senior sector of the current globalization (as capitals initiated, thanks to computerization, the speed up of the current globalization process). Secondly, in the case of the cultural industries, to which the mass media are integrated, the impact has also been severe and manifold: extra-corporative (outside the corporation, in the marketplace) and intra-corporative (in routines and work practices inside the corporation), on the one hand; but also in the channel, message, production means and consumption, on the other hand. In both cases, either in the context of the media or in the financial sector or in any other sector, the arrival of ICT during the second half of the 20th century has been accompanied by a tremendous expectation. Their potential is enormous, whether from a material and economic or an intellectual and social point of view. This expectation is for instance articulated in World Bank studies. In a report from December 2003, the World Bank dared to put figures at the growing link between ICT and economic growth (The World Bank, 2004). This meant and still means a double link, according to the World Bank: the increasing production of ICT contributes to a growth in production, employment and export; meanwhile, the use of ICT increases productivity,

competitiveness and economic growth as well. That is, these new technologies generate wealth as an industrial sector by themselves, and they contribute at the same time to an increase in the wealth of the sectors that use them. The World Bank does not pinpoint whether this technological race and economic growth are the solutions to the problems of humanity (though it acknowledges that the contribution from ICT to the economic growth of developing countries is still limited) . However, the World Bank report concludes with an interesting sentence about the positive effect of ICTs on global economic development:

Its applications provide access to worldwide information and allow for collaboration amongst people from different continents. Greater access to information and opportunities for collaboration can create job opportunities, transfer of skills, and greater efficiency and transparency in politics and business (The World Bank, 2004: 23). This is the point. New ICTs have an additional potential, which is as encouraging as it has hardly been exploited: its enormous possibilities for increasing transparency of political and economic management of social agents. This greater management transparency could become the biggest step forward ICT might provide to our current society. ICT could become a democratizing instrument not only regarding the globalization of knowledge but also in the fight against fraud. More than two hundred years ago, Immanuel Kant defined transparency (publicity) as a useful instrument to measure justice of the acting principles in his work Perpetual Peace. 'Thus the principle of incompatibility between the maxims of international law and publicity provides a clear example of the nonconformity of politics to morality (as a, science of right)', as stated in regards to the theory of law (Kant, 1795). We could apply the same principle to the economic theory: a transparent economic management is not automatically fair and right but an economic administration afraid of publicity can hardly be fair and right. New ICT that enable a maximum of transparency can provide a check on the fairness of our systems. However, this publicity and by implication democratizing potential of ICT is vastly wasted. Instead, all the attention and effort is concentrated towards their more economical side, such as the ability for spurring productivity and corporative profits.

Indeed, digitalization has affected in full the nature of all productive sectors, their corporate structures, and the way people belonging to these sectors work. One of the most outstanding effects derived from that is the increasing business concentration and the increasing competition and productivity. But the question that nobody asks is: where have the potential effects of ICT in the increase of transparency gone? The increase in transparency in the economic management referred to by the World Bank is one of the central elements in the assumed democratizing role of ICT. This greater transparency would have been possible by means of two factors which usually characterize the digital revolution, and a third aspect far less explained. These are:

Firstly, and this is repeated ad nauseam, the greater volume of information available in this digital era means by itself an increase in transparency. And this is mainly true for

both public and private organizations, whose data used to be available only in a physical carrier and at one point in time, have increased the volume of information by uploading their relevant corporate information into the Internet (specially legal filings as annual reports, fiscal years statements and forms, stock info, financial and corporate history). Secondly and equally endorsed, transparency increases not only by the greater volume of available information, but also by the greater amount of agents with access to that information, restricted in the past to a few channels and target groups.

And thirdly, and vastly underestimated, the computerization of the public and private spheres that massively happened since the 1980s involved an exponential increase in the control of information. Hence in turn, the public control of the private sphere. It also greatly increased the complexity of the functioning of the information systems, but that price was worth paying, or at least it seemed right, taking into account all the benefits: for the public sector it meant a greater control of the obligations of the private sector, and for this last one, it involved a tremendous simplification and improvement of its working procedures, and most important, a considerable reduction in costs. With digitalization everything is faster and better. And everything leaves a record, even the attempts to remove this record. To the above, numerous weak points will later be added. The increase in the amount of information becomes an oversaturation which can become disinformative; the greater availability faces a huge gap not only in the access to information but also in the knowledge required to make this access effective; and globalization hinders any control over transnational corporations. But this ICT potential does exist and it is in this greater transparency that its attributed important democratizing function is based. However, and that is the key point in our argument, this democratizing role constitutes now a fraud, because, in practice, the benefits of ICT are being more used (or at least as used) to escape the democratic control than to guarantee it.

Financial crime and the lack of transparency

It is widely known that the first phase in the speeding up of world globalization during the second half of the 20th century was the globalization of capital. According to many people, that is the proper definition of globalization. For instance: [Globalization or internationalization] is defined as the progressive process of integration of the national economies into the world market framework. A process of liberalization of exchanges and international movements of capital; a continuation of the old progressive liberalization trends for external exchanges, abruptly interrupted at different times in history by the success of protectionist ideas (Suárez Suárez 2001:2). What makes this possible? There are here two issues, essentially. The first one is the political will, dramatized with the arrival of conservative leaders to the government in financially stronger countries. Such leaders advocated for the need to restore free trade, which they unfailingly associated with economic prosperity (essentially Reagan in the USA and Thatcher in the UK). The second issue is the exponential growth of technological development, essentially in the context of communications and transport, experienced in the most developed countries. We can find other reasons such as the role of the World

Trade Organization, multinationals, and the worldwide acceptance of North American culture, but none of these are as relevant as the previous two ones. And the first wave of globalization that the new technologies do accelerate is the one that affects the financial markets. Global capitalism started in the 70s. Oil producing countries joined into the Organization of the Petroleum Exporting Countries (OPEC), and raised the price of crude oil. These countries suddenly faced substantial commercial surplus. The responsibility for recycling these petrodollars laid on the Western commercial banks with the approval and unspoken help of their respective governments. The Eurodollar market was then born, or rather, it experienced an extraordinary push, and with it, the first serious experiment of internationalization of the financial markets took place (Suárez Suárez 2001:8-9). This internationalization of the financial system at such a speed and scope would have been completely impossible without new ICT. But the greater speed, connection and data control that ICT allowed was not exploited, paradoxically, to create a more transparent system essential for legal business, but rather, to escape from the transparency itself. Indeed, the phenomenon of capital internationalization in such a way accelerated, but not initiated, in the 70s was going to experience an unprecedented splitting at the same time when a new system parallel to the legitimate one was born: tax havens.

Tax haven is the popular denomination by which the offshore financial centers are known, where ‘offshore’ is an euphemism for ‘located in a lawless land’ (or with a relaxed legal regime) (Hernández Vigueras, 2005). Tax heavens --- also born in the 70s --- peaked around the 1980’s, this peak being associated to the suppression of legal impairments, exchange controls, and the development of telecommunications, which have intensified the international movements of financial capitals. Their growth has been fostered by the flows of digital information which allow the easy and inexpensive transfer of money and data in real time (Hernández Vigueras, 2003). According to Ramón Tamames, a tax haven is a land with a ‘tax regime that favors foreign residents and local societies with low or non-existent taxes’ (Tamames, 2002). In 2000, the Organization for Economic Co-operation and Development (OECD), after years of work, identified 35 countries and territories which should be considered tax havens (OECD, 2000). This figure would increase and change later on, depending on the classifying organizations and according to a degree of permissiveness. The absolute permissiveness is found in countries such as the Bahamas, Caiman Islands, British Virgin Islands, where neither financial audits nor presentation of accounts in any public office are required, nor the communication of profits or the identification of the society's managers and/or shareholders. There, the legislation to repress transactions and laundering of money arising from crime is only recent. Less permissive tax havens are Andorra, Barbados, Jamaica or Monaco, where specifications of obtained profits, the register of social accounts in public registries and the compulsory identification of the managers, are all now required . After many hindrances --- due to the opposition of many countries ---, at the end of the 1990s a group of strong countries within the OECD agreed that offshore territories serve essentially to tax evasion and capital laundering. In particular, investment Bank Merrill Lynch estimated in their report World Wealth Report (2002) that in 2001

one third of the world wealth was kept in tax havens; i.e. $ 8.5 trillion from a total of $ 26.2 trillion of financial assets belonging to the great world fortunes (Merrill Lynch, 2002: 2 and 11). Considering that Merrill Lynch estimates are regarded as conservative by anti-white collar crime organizations, the evolution of this phenomenon is worrying. Even more if we look at the recent past, as these estimations have been continuously increasing. Merrill Lynch calculated the capitals in offshore financial centers as $ 6 trillion in 2000 (Komisar, 2003) and other sources estimated $ 5 trillion deposits in 1998 (Pedrero 2004: 155). The role of the banking system in this phenomenon is also clearly visible within the sector records themselves. In 2000, Merrill Lynch calculated that at least half of the $ 6 trillion located in offshore centers was placed in banks located in tax haven countries (Merrill Lynch, 2001). That is, according to the estimations of the banking system, a third of the financial assets of high net worth individuals (people with more than $1 million in financial asset wealth) can be found offshore, and banks manage at least half of them. Financial entities have thousands of branches sited in tax havens. Most of these are not offices from unknown banks, but delegations or branches belonging to the world's main financial companies. Jean Ziegler describes the main thoroughfare of Nassau, home town to more than half of the population of Bahamas:

The offices of hundreds of IT professionals, audit specialists, financial analysts, lawyers and notaries are located along the main street of Nassau. These professionals are the foundations of this offshore haven. Amongst them there are around 300 Swiss citizens, who are mostly directors or employees from one of the thirty-four Swiss banks managing businesses for the most important and selected clients (Ziegler, 2002).

In summary, this is a problem of great dimensions mainly sustained for political reasons. A real determination to finish with them does not exist, on the contrary, there are voices in favour, as well as technical reasons for which their existence is only possible thanks to ICT and the lack of transparency in their use. Herbert Schiller already forecasted many years ago:

Those who believe state power will be enhanced with the new information technologies and expanded information flows may be overlooking one critical point. The main, though not exclusive, beneficiaries of the new instrumentation and its product, already are the powerful global corporations. As they have done in the past, they will be the first to install and use these advanced techniques. In fact, they have been doing so for some time (Schiller, 1996:103). There is no doubt that financial companies are at the head of these ‘powerful global corporations’. It is possible, then, to state that new technologies have been, and still are, working in the service of the greatest possible profit operated by agents whose final objective is to evade legislations with poorly liberalized tax systems. However, to speak about difficulties in the control of capital movement, and the impossibility to control movements, transactions and intangible flows can only be an ignorance-related fickleness. Nothing is more tangible that the electrical impulse which forms the digital bit of information itself. Indeed, ICTs (essentially computing and

telecommunications) which set up electronic banking transactions in the second half of the 20th century did not subsume the banking system within the virtual shadows. Instead, they put the very key to transparency in our hands. The fact that all the transactions are conducted electronically does not mean they can be hidden from public opinion, but that they are under a greater control; an absolute control in fact. Nowadays everything remains recorded in electronic registries. Although these electronic registries can be erased, manipulated or altered, this is at the expense of leaving a footprint. Never before has a similar tool to control such complex systems been available. Therefore, fraud is anything but innocent, as will be seen next when we discuss financing.

The Role of ICT in fraud: The clearing case

It is not a paradox but common sense, that the same technology which allows parallel opaque financial systems to exist, may be the key to change this state of affairs. This is the main lesson to extract from an important investigation embodied in two books that have had hardly any impact on the public opinion: Révélations (Revelations) (2001) and La boîte noire (The Black Box) (2002). Both books are written by French researcher and journalist Denis Robert, who describes a long and dense investigation proving, amongst other things, that the weakness of the criminal financial system stems from the very strength of the system --- that is, from ICTs use. To understand this we must first talk about contemporary history of the financial systems and the meaning of clearing. During the early 1970's, several banks established around the world decided to associate and set up an interbanking cooperative. At that time they were only a hundred (today they add up to more than two thousand) and their objective was to create a system to facilitate international banking exchanges, which would be called clearing. Denis Robert explains it in this way:

Let’s go back some decades. When an insurance agent from Chicago wanted to sell part of his company's capital to a Greek shipowner, how did he do it? He went to see his banker, let's say the Bank of New York, and confided to him the task of selling the bonds. The banker took a plane to Athens, where he was going to meet with the shipowner’s banker, for instance the Greek subsidiary of the ABN AMRO Bank. Clearing allows, on one hand, to save time, and therefore, money. It is not necessary to travel. From then on, a central organization has guaranteed the happening of the exchange. The basic principle is trivial: bankers from different countries should join to create a confidence area where the banking exchange will be registered and guaranteed. Unlike the stock exchange market, which brings together the different elements of a transaction, a clearing company is an infrastructure apparently passive. It takes care of registering and guaranteeing the modification. The bonds do not move, only the name of the owner is changed (Robert, 2001:22-23). The clearing system, also known as ‘compensation systems’, pretended to bypass the minimum two weeks which the foreign buyer had to wait before the bonds arrived (for instance, a Rome bank buying IBM shares from a bank in New York, as requested by a client). It was aimed at avoiding time and money costs (the shipment had to be insured, and precious time was wasted while the bonds were physically travelling).

The first clearing society, Euroclear , was created in 1968 in Brussels and was founded by an American bank, Morgan Guaranty Trust Company of New York, which at the time was the biggest private bank in the world.

The second clearing society appeared in 1970, called Cedel (now Clearstream) , as a reaction from the European or American banks who had not participated in the creation of the first clearing society. These are, until now, the two only current transnational clearing societies. Euroclear and Clearstream allow their member institutions to exchange titles (shares, securities, and the like) to balance their accounts after performing operations at their own risk or on behalf of their clients. Their success was such that all current important international transactions are now dealt through one of these two societies exclusively. A compulsory step that involves 'the almost real time recording and storing of a footprint of a transaction in codified documents' (Robert, 2001:24). Although these are the only two clearing systems at a cross-border level in the world, clearing systems exist at the national level almost in any country. Their tasks are limited to domestic compensatory operations of capital exchange, and the amounts of money shifted around by the national societies cannot be compared at all to those of the international societies. In December 2004, Clearstrem alone claimed to be performing 250,000 transactions daily (the total number of international transactions processed by Clearstream rose to 17.2 million throughout 2004), while the value of assets held in custody on behalf of customers rose to approximately EUR 7.6 trillion. In summary, since the 1970s, clearing 'has learned to make itself discretely essential' (Robert, 2001:40), and has been progressing in close association with economic liberalization. 'Clearing has contributed to the foundation of what economy and financial journalists have christened as the Global Village (much later after bankers and clearing users adopted Marshall McLuhan's term). A Village where power and information centers are interconnected' (Robert, 2001:41). Currently, there is no important international transaction that is not channeled through one of these two big companies, Euroclear and Clearstream. The clearing system has become, by mouth of an ex-official of Clearstream, 'the world's notary' (Robert, 2001:244). Sure enough, the rulers of the clearing societies are the new world's digital notaries. Every single international or national financial transaction is registered there, and anyone trying to avoid the clearing societies risks ending up outside the world's banking system. That is, international clearing systems are the mechanisms of mutual confidence created by banks so they have a chance to play on the world's financial field. It is an organized system that has accompanied the explosion of financial markets, and here you have the big discovery by Denis Robert: clearing has superbly adjusted to the interest of some key groups. Robert, with the help of an insider from one of the two big cross-border clearing societies, Ernest Backes, co-author of one of his books, concludes that these systems are an ideal method for money hiding and laundering, and that it is in this way how they are being used. Thanks to a perversion of the clearing systems --- states Robert --- fraud opportunities at the international level are made much easier, making them practically undetectable. But, even if undetectable and invisible for public control, they are still existing and can be prosecuted. Robert and

Backes describe details for this with a wealth of evidence. They reveal how both clearing societies use the undisclosed accounts system (created for a particular legitimate use) to hide certain transactions. Transactions carried out in these undisclosed accounts represent, according to Robert and Backes, a tremendous opportunity for those seeking 'maximal discretion in the global village' and succulent profits for the clearing society. Further, they state:

It has been established that most of the accounts managed from tax havens, especially those from large European and American banks, are undisclosed accounts. We can interpret this as the search for maximum discretion, in this way, a double security lock. Not only do they create a subsidiary in a tax haven, but they also provide it with undisclosed accounts (Robert, 2001: 206-207).

In summary, both researchers claim that clearing societies, other than being used for the objectives they were intended --- to facilitate international transactions, thus providing the conditions for financial and economic globalization by the end of the 1990s --- are additionally used as a means for organized crime. For this unit, the importance of the work published by Robert and Backes does not lie in its explicit accusation but on the warning that is implicitly derived from it: that the same conditions allowing global fraud are the very ones that facilitate fighting it.

Indeed, although Clearstream and Euroclear were created to speed up the exchange of equities and to avoid the physical transfer of titles and money, this would have not been possible without the fundamental role of ICTs. Essentially, computing and telecommunications enabled the creation of clearing societies, which in turn guarantee their management. All clearing societies keep records of every single transaction performed. Even if pretending not doing so, it would be absurd, as this is their safety guarantee against their most influential clients. It is the use of this sophisticated technology that makes these societies trustworthy; it is precisely their technology that allows managing the complexity of the system and keeping it under control. Any judicial or criminal inquiry about international crime would be able to progress drastically if it would have open access to the registries of these two big societies. ICTs are related to such a degree to the creation and maintenance of the financial world core that the main instrument of these clearing societies is itself a technology company: The Society for Worldwide Interbank Financial Telecommunication (SWIFT). SWIFT was created by the main shareholders of the two international clearing systems (a group of 239 European and North-American banks) in Belgium in 1973. Currently, it belongs to more than 3,000 banks and connects more than 7,600 financial institutions. The aim of creating SWIFT was to provide clearing societies with an instrument for extra fast transmission of cash in every currency.

Nowadays, nearly all the banks in the world are connected by means of this system. SWIFT is the technology platform that links all the world's financial institutions and that

is used by the two big clearing societies. According to data from the company itself , in 2004 the SWIFT world network transferred several billion dollars a day for the 3.5 million messages negotiated daily (which meant more than 2,000 million messages negotiated that year). And, anything can be found in the SWIFT channels, 'from a Serbian dictator's bank to that of an Iraqi chemical weapons dealer, including the investment society of a Colombian dealer or the broker company from a Panamian shipowner' (Robert, 2001:42-43). However, the clearing societies and SWIFT are not the only link in the chain for those wanting to launder money. An accomplice entry bank that is ready to risk accepting doubtful funds must be involved. But this is not a problem thanks to tax havens. Robert goes further in stating that 'tax havens would not exist without large trading banks and without the international clearing societies belonging to these large trading banks' (Robert, 2001: 252). He adds to this that the growth of offshore systems is nearly paralleled by the growth of the clearing system: Nowadays, most of the literature in this subject report up to at least fifty per cent of the world financial movements as circulating through tax havens. The comparison with the increase in power of the international clearing is surprising (Robert, 2001:251).

According to this investigator:
The dreadful couple "international clearing-banking haven" offers extra protected opacity pockets only accessible to the initiated: secret services or ministries, but mostly, banks, multinational companies, turbid companies... (Robert, 2001: 259-260).

In short, ICTs enable reliable and safe interconnection of finances around the world. But this interconnection belongs to the private hands of the interconnected agents themselves, which has led to 'unsustainable diversions to the detriment of transparency in the markets' (Robert, 2001:261). The pretended self-regulation of the financial markets and the agreements amongst some large banks and multinational companies, trying to hide their benefits, has added to the substantial profits arising from managing gains related to terrorism and drug dealing. This has led to the perversion of the system which, still working for its legitimate original purpose, has suffered an illicit broadening of its uses. But, at the same time, clearing societies offer an ideal point of view: they are the perfect vantage point over the financial markets. A popular argument amongst politicians and economists regarding organized crime, and more specifically, financial crime, is the impossibility to control world transactions. This is the main reason why, for instance, critics of the Tobin Tax consider it impossible to apply. However, the ad fundum knowledge of the real function of financial markets leads to quite different conclusions: it is perfectly possible (and relatively easy) to accurately quantify the daily value of international financial transactions. The reason being as much technical as corporative. The most important financial transactions are cleared and recorded electronically by only two international clearing societies (the national transactions are in the corresponding national clearing societies). The reliability and accuracy of such exchanges has to be guaranteed, otherwise the system would not be safe and reliable enough to be used by its own users and clients. Therefore, it should not be a problem to claim a tax for

international transactions, to control the main financial movements in the world, or to ascertain the whereabouts of large sums of vanished money, as long as the international clearing system made its technological platform accessible to magistrates, the police, politicians and citizens. When a journalistic source speaks about an enormous volume of illegal or crime related money that is vanished and that evades justice, what this source should rather talk about is money 'protected within the opacity' in which clearing societies work. Money is not evaded, what has been evaded are legal responsibilities. The reason is simple: clearing --- the real functioning of the markets, the technological foundation for world finances --- is an absolute unknown.

The role of the mass media and the financial and digital illiteracy

The macro and micro keys determining the ups and downs of financial markets are a subject of continuous debate amongst financial and economic experts who try to explain the present and foresee the future for our economy. Theories are common; as are conjectures, speculations and hypotheses surrounding these theories. These are the basis of predictions considered impossible by some. However, nobody tackles the technical approach, the real functioning of the financial system engine.

On the contrary, the financial world is, to the collective mind, a vague, diffuse and far away scenario, where some distant agents make decisions, forecast events and give accounts for facts that most people do not understand. This majority of people though, does include those who are supposed to understand better: judges, magistrates, politicians, researchers, security bodies... Few of them have ever heard about clearing, and amongst them, even fewer understand its real functioning. And the same happens in the field of communication networks. Economics expert Jean Ziegler mentioned in one of his most critical works against the financial system the technical impossibility of controlling the identity of the capitals in constant migration, due to the easiness offered by the cyberspace. The digital scenario is still intangible and elusive for many. In fact, both worlds, of finance and digital technology, suffer from the same problem: their degree of complexity requires a high level of comprehension and competence. A further step which only a few are willing to take. Therefore, we could say that there is a popular illiteracy, or if one prefers, a total lack of interest for these issues --- considered mere technical issues for the outsiders. This lack of interest and knowledge could be boosted by the financial system itself. 'In the financial community, secrecy is considered natural' states former World Bank Senior Vice President and Chief Economist Josep Stiglitz. Clearing societies --- that is, the main financial institutions and the most important world corporations controlling clearing --- are not interested in anyone able to interfere in their control. For the reasons stated in this article it can be easily deduced that such international mechanisms should be under democratic control.

Self Assessment Exercise

In summary, both researchers claim that

1. How do clearing societies, used as a means for organized crime?
2. Explain the idea behind the argument that 'the same conditions allowing global fraud are the very ones that facilitate fighting it.

4.0 Conclusion

It is however important to state that we need, thus, to reconsider what we are using the ICTs for, and reliably redirect these towards solidarity, democracy and justice. The current technological fraud is everything but innocent. Over the years, financial speculation and war have monopolized the main ICTs resources and ICTs investment in the world. Whenever there is a crisis or there are stock exchange scandals ruining thousands of people, or natural disasters like the Indian tsunami, the blame goes to the unforeseeable forces of nature (whether human or environmental). But for some of the countries devastated by the tsunamis, there was a margin of hours to warn the population. However, the lack of the necessary communication systems and logistics prevented making use of this time. Now it is time that the media explains that the uses these centers of power are making of ICTs are not always legitimate. And that we can efficiently fight against this; a possibility that is kept hidden from us again and again. This constitutes the big fraud.

5.0 Summary

The democratizing dimension of the new information system security management, and communication technologies (ICTs) is a widely accepted proposition. Although this is repeatedly emphasized and explained by economic, political and social theories that deal with the analysis of the Information Society, a good deal of its significance has been systematically neglected. ICTs are exclusively approached either from the perspective of the globalization of knowledge or from the perspective of economic productivity.

6.0 Tutor Marked Assignment

What are the role of the mass media in financial and digital illiteracy?

7.0 References/ Further Reading

BACON, Francis (1597): Meditationes Sacræ. De Hæresibus [Religious Meditations, Of Heresies].

BOSWORTH, B.P. and TRIPLETT, J.E. (2000): 'What's new about the New Economy? It, Economic Growth and Productivity', Brookings Economic Papers, October 20.

BUSH, V. (1945): 'As we may think', Athlantic Monthly, July, Volume 176, No. 1; 101-108.

CARNOY, M. et al. (1993) The New global Economy in the Information Age, University Park: Pennsilvanian State University Press.

CASTELLS, M (1997): The Information Age: Economy, Society and Culture (3 volumes), Cambridge, Massachusetts: Blackwell publishers Inc.

CLEARSTREAM (2004): ‘Deutsche Börse Group Annual Report 2003’, under: http://www.clearstream.com.
DE KERCKHOVE, D. (1995): The skin of culture, Toronto: Somerville House Books.
GALBRAITH, John Kenneth (2004): The economics of innocent fraud: Truth for our time, Boston: Houghton Mifflin.
GRAHAM, Gordon (1999): The Internet : a philosophical inquiry, London/New York: Routledge.
HERNÁNDEZ VIGUERAS, Juan (2005): Los paraísos fiscales (Tax heavens), Spanish, Madrid: Akal.HERNÁNDEZ VIGUERAS, Juan (2003): Los paraísos fiscales: un subproducto de la globalización liberal
(Tax heavens: a subproduct of liberal globalization), Spanish, Attac, March 2003, under http://www.attacmadrid.org.
HIMANEN, Pekka (2001): Hacker ethic, and the spirit of the information age, New York: Random House.
IMF (2000): ‘Offshore Financial Centers IMF Background Paper’, New York : International Monetary Fund, 23 june.
JONES, C.I. (1995a): ‘Time Series Tests of Endogenous Growth Models’, Quarterly Journal of Economics, 110, pp.495-525.
JONES, C.I. (1995b): ‘R&D-Based Models of Economic Growth’, Journal of Political Economy, 103, pp.759-784.
KANT, Immanuel (1795): Perpetual Peace : a philosophical essay, At:
http://www.constitution.org/kant/perpeace.txt.
KATZ, Raul L. (1988): The Information Society: an International Perspective, Nova York: Praeger.
KOMISAR, Lucy (2003): ‘Offshore Banking: The Secret Threat to America‘, Disent Magazine, under: http://www.dissentmagazine.org/menutest/articles/sp03/komisar.htm.
KOVACH, B. Y ROSENSTIEL, T. (2001): The Elements of Journalism: what news people should know and the public should expect, New York: Crown Publishers.
LE MONDE DIPLOMATIQUE (2000): Pensamiento crítico vs. Pensamiento único (Critical though vs Unique Though), Spanish, Madrid: Debate.
LESSIG, Lawrence (1999) : Code and other laws of cyberspace, New York: Basic Books.
LOO, Ivo and SOETE, Luc (1999) : ‘The Impact of Technology on Economic Growth: Some New Ideas and Empirical Considerations’, Research Memoranda 017, Maastricht:

UNIT 2
An overview of Information Security as a risk management function

Content

1.0 Introduction

Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions. This process is not unique to the IT environment; indeed it pervades decision-making in all areas of our daily lives. Take the case of home security, for example many people decide to have home security systems installed and pay a monthly fee to a service provider to have these systems monitored for the better protection of their property. Presumably, the homeowners have weighed the cost of system installation and monitoring against the value of their household goods and their family's safety, a fundamental "mission" need. The head of an organizational unit must ensure that the organization has the capabilities needed to accomplish its mission. These mission owners must determine the security capabilities that their IT systems must have to provide the desired level of mission support in the face of real world threats. Most organizations have tight budgets for IT security; therefore, IT security spending must be reviewed as thoroughly as other management decisions. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities.

2.0 Objectives

Students are expected to understand

1. the concept of Risk management as a management responsibility and
2. the key roles of the personnel who should support and participate in the risk management process.

3.0 Main body

Integration of Risk Management into SDLC

Minimizing negative impact on an organization and need for sound basis in decision making are the fundamental reasons organizations implement a risk management process

for their IT systems. Effective risk management must be totally integrated into the SDLC. An IT System Development Life Cycle (SDLC) has five phases: initiation, development or acquisition, implementation, operation or maintenance, and disposal. In some cases, an IT system may occupy several of these phases at the same time. However, the risk management methodology is the same regardless of the SDLC phase for which the assessment is being conducted. Risk management is an iterative process that can be performed during each major phase of the SDLC.

Table1. Describes the characteristics of each SDLC phase and indicates how risk management can be performed in support of each phase.

SDLC Phases	Phase Characteristics	Support from Risk Management Activities
Phase 1—Initiation	The need for an IT system is expressed and the purpose and scope of the IT system is documented	• Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations (strategy)
Phase 2—Development or Acquisition	The IT system is designed, purchased, programmed, developed, or otherwise constructed	• The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design trade-offs during system development
Phase 3—Implementation	The system security features should be configured, enabled, tested, and verified	• The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to system operation
Phase 4—Operation or Maintenance	The system performs its functions. Typically the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies, and procedures	• Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whenever major changes are made to an IT system in its operational, production environment (e.g., new system interfaces)
Phase 5—Disposal	This phase may involve the disposition of information, hardware, and software. Activities may include moving, archiving, discarding, or destroying information and sanitizing the hardware and software	• Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner

KEY ROLES

Risk management is a management responsibility. This section describes the key roles of the personnel who should support and participate in the risk management process.

• **Senior Management.** Senior management, under the standard of due care and ultimate responsibility for mission accomplishment, must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. They must also assess and incorporate results of the risk assessment activity into the decision

making process. An effective risk management program that assesses and mitigates IT-related mission risks requires the support and involvement of senior management.

• **Chief Information Officer (CIO).** The CIO is responsible for the agency's IT planning, budgeting, and performance including its information security components. Decisions made in these areas should be based on an effective risk management program.

• **System and Information Owners.** The system and information owners are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own. Typically the system and information owners are responsible for changes to their IT systems. Thus, they usually have to approve and sign off on changes to their IT systems (e.g., system enhancement, major changes to the software and hardware). The system and information owners must therefore understand their role in the risk management process and fully support this process.

• **Business and Functional Managers.** The managers responsible for business operations and IT procurement process must take an active role in the risk management process. These managers are the individuals with the authority and responsibility for making the trade-off decisions essential to mission accomplishment. Their involvement in the risk management process enables the achievement of proper security for the IT systems, which, if managed properly, will provide mission effectiveness with a minimal expenditure of resources.

• **Information system security officer (ISSO).** IT security program managers and computer security officers are responsible for their organizations' security programs, including risk management. Therefore, they play a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize risks to the IT systems that support their organizations' missions. ISSOs also act as major consultants in support of senior management to ensure that this activity takes place on an ongoing basis.

• **IT Security Practitioners.** IT security practitioners (e.g., network, system, application, and database administrators; computer specialists; security analysts; security consultants) are responsible for proper implementation of security requirements in their IT systems. As changes occur in the existing IT system environment (e.g., expansion in network connectivity, changes to the existing infrastructure and organizational policies, introduction of new technologies), the IT security practitioners must support or use the risk management process to identify and assess new potential risks and implement new security controls as needed to safeguard their IT systems.

• **Security Awareness Trainers (Security/Subject Matter Professionals).**

The organization's personnel are the users of the IT systems. Use of the IT systems and data according to an organization's policies, guidelines, and rules of behaviour is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, it is essential that system and application users be provided with security awareness training. Therefore, the IT security trainers or security/subject matter professionals must understand the risk management process so that they can develop appropriate training materials and incorporate risk assessment into training programs to educate the end users.

Self Assessment Exercise
Discuss the concept of Risk management as a management responsibility.

4.0 Conclusion
To minimize risk to the IT systems, it is essential that system and application users be provided with security awareness training. Therefore, the IT security trainers or security/subject matter professionals must understand the risk management process so that they can develop appropriate training materials and incorporate risk assessment into training programs to educate the end users.

5.0 Summary
This unit describes the characteristics of each SDLC phase and indicates how risk management can be performed in support of each phase. It further explains risk management as a process that allows IT managers to balance the operational and economic costs of protective measures, and how best to minimise risk in IT system.

6.0 Tutor Marked Assignment
List and discuss the phases in IT System Development Life Cycle (SDLC).

7.0 References/Further Reading

Computer Systems Laboratory Bulletin. *Threats to Computer Systems: An Overview*. March 1994.

NIST Interagency Reports 4749. *Sample Statements of Work for Federal Computer Security*
Services: For Use In-House or Contracting Out. December 1991.

NIST Special Publication 800-12. *An Introduction to Computer Security: The NIST Handbook*. October 1995.

NIST Special Publication 800-14. *Generally Accepted Principles and Practices for Securing*
Information Technology Systems. September 1996. Co-authored with Barbara Guttman.

NIST Special Publication 800-18. *Guide For Developing Security Plans for Information Technology Systems*. December 1998. Co-authored with Federal Computer Security Managers' Forum Working Group.

NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*. August 2001.

NIST Special Publication 800-27. *Engineering Principles for IT Security*. June 2001.
OMB Circular A-130. *Management of Federal Information Resources.* Appendix III. November 2000.

UNIT 3

RISK ASSESSMENT

Content

1.0 Introduction

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its SDLC. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process. *Risk* is a function of the *likelihood* of a given *threat-source's* exercising a particular potential *vulnerability*, and the resulting *impact* of that adverse event on the organization.

2.0 Objectives

Students are expected to understand the various concepts such as vulnerability, threat sources, level of impact, IT system components and data and other risk assessment activities. Secondly at the end of this unit they should be able to appraise vulnerability in an IT system using the nine primary steps in risk assessment methodology.

3.0 Main body

To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system. Impact refers to the magnitude of harm that could be caused by a threat's exercise of a vulnerability. The level of impact is governed by the potential mission impacts and in turn produces a relative value for the IT assets and resources affected (e.g., the criticality and sensitivity of the IT system components and data). The risk assessment methodology encompasses nine primary steps, which are described below:

Step 1: System Characterization
Step 2:Threat Identification

Step 3:Vulnerability Identification
Step 4:Control Analysis
Step 5:Likelihood Determination
Step 6:Impact Analysis
Step 7:Risk Determination
Step 8:Control Recommendations
Step 9:Results Documentation
Steps 2, 3, 4, and 6 can be conducted in parallel after Step 1 has been completed. Figure 1 depicts these steps and the inputs to and outputs from each step.

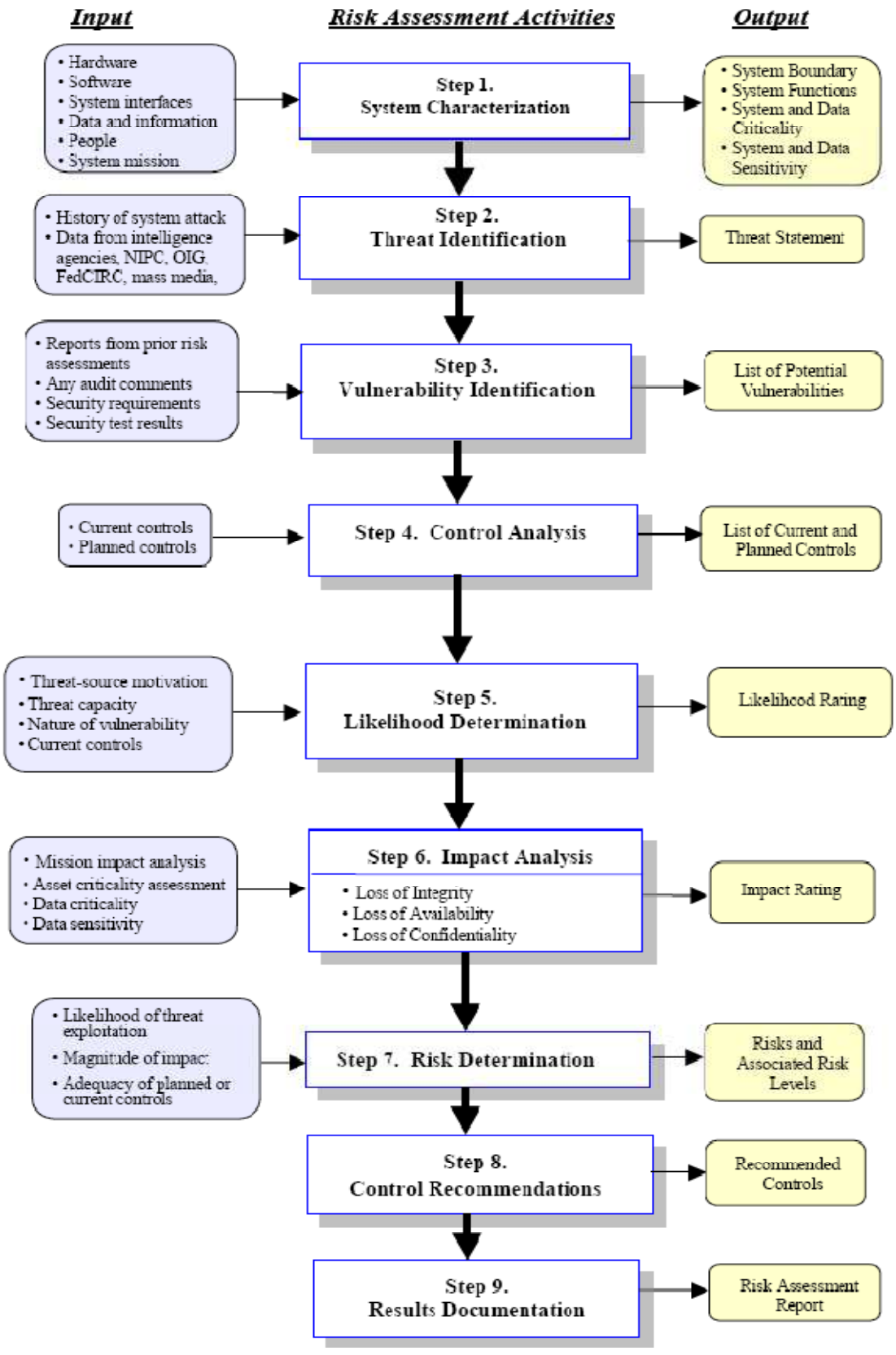

Input
Risk Assessment Activities
Output
• Hardware
• Software
• System interfaces
• Data and information
• People
• System mission
Step 1.
System Characterization
• System Boundary
• System Functions
• System and Data Criticality
• System and Data Sensitivity
• History of system attack
• Data from intelligence agencies, NIPC, OIG, FedCIRC, mass media,
Step 2.
Threat Identification
Threat Statement
• Reports from prior risk assessments
• Any audit comments
• Security requirements
• Security test results
Step 3.
Vulnerability Identification
List of Potential Vulnerabilities
• Current controls
• Planned controls
Step 4. Control Analysis
List of Current and Planned Controls
• Threat-source motivation
• Threat capacity
• Nature of vulnerability
• Current controls
Step 5.
Likelihood Determination
Likelihood Rating
• Mission impact analysis
• Asset criticality assessment
• Data criticality
• Data sensitivity
Step 6. Impact Analysis
• Loss of Integrity
• Loss of Availability
• Loss of Confidentiality
Impact Rating
• Likelihood of threat exploitation
• Magnitude of impact
• Adequacy of planned or current controls
Step 7. Risk Determination
Risks and Associated Risk Levels
Step 8.
Control Recommendations
Recommended Controls
Step 9.
Results Documentation
Risk Assessment Report

Figure1. Risk Assessment Methodology Flowchart

STEP 1: SYSTEM CHARACTERIZATION

In assessing risks for an IT system, the first step is to define the scope of the effort. In this step, the boundaries of the IT system are identified, along with the resources and the information that constitute the system. Characterizing an IT system establishes the scope of the risk assessment effort, delineates the operational authorization (or accreditation) boundaries, and provides information (e.g., hardware, software, system connectivity, and responsible division or support personnel) essential to defining the risk. Section 1.1 describes the system-related information used to characterize an IT system and its operational environment. Section 1.2 suggests the information-gathering techniques that can be used to solicit information relevant to the IT system processing environment. The methodology described in this document can be applied to assessments of single or multiple, interrelated systems. In the latter case, it is important that the domain of interest and all interfaces and dependencies be well defined prior to applying the methodology.

1.1 System-Related Information

Identifying risk for an IT system requires a keen understanding of the system's processing environment. The person or persons who conduct the risk assessment must therefore first collect system-related information, which is usually classified as follows:

- Hardware
- Software
- System interfaces (e.g., internal and external connectivity)
- Data and information
- Persons who support and use the IT system
- System mission (e.g., the processes performed by the IT system)
- System and data criticality (e.g., the system's value or importance to an organization)
- System and data sensitivity.

Additional information related to the operational environment of the IT system and its data includes, but is not limited to, the following:

- The functional requirements of the IT system
- Users of the system (e.g., system users who provide technical support to the IT system; application users who use the IT system to perform business functions)
- System security policies governing the IT system (organizational policies, federal requirements, laws, industry practices)
- System security architecture
- Current network topology (e.g., network diagram)
- Information storage protection that safeguards system and data availability, integrity, and confidentiality
- Flow of information pertaining to the IT system (e.g., system interfaces, system input and output flowchart)

• Technical controls used for the IT system (e.g., built-in or add-on security product that supports identification and authentication, discretionary or mandatory access control, audit, residual information protection, encryption methods)
• Management controls used for the IT system (e.g., rules of behaviour, security planning)
• Operational controls used for the IT system (e.g., personnel security, backup, contingency, and resumption and recovery operations; system maintenance; off-site storage; user account establishment and deletion procedures; controls for segregation of user functions, such as privileged user access versus standard user access)
• Physical security environment of the IT system (e.g., facility security, data centre policies)
•Environmental security implemented for the IT system processing environment (e.g., controls for humidity, water, power, pollution, temperature, and chemicals). For a system that is in the initiation or design phase, system information can be derived from the design or requirements document. For an IT system under development, it is necessary to define key security rules and attributes planned for the future IT system. System design documents and the system security plan can provide useful information about the security of an IT system that is in development. For an operational IT system, data is collected about the IT system in its production environment, including data on system configuration, connectivity, and documented and undocumented procedures and practices. Therefore, the system description can be based on the security provided by the underlying infrastructure or on future security plans for the IT system.

1.2 Information-Gathering Techniques
Any, or a combination, of the following techniques can be used in gathering information relevant to the IT system within its operational boundary:

• **Questionnaire.** To collect relevant information, risk assessment personnel can develop a questionnaire concerning the management and operational controls planned or used for the IT system. This questionnaire should be distributed to the applicable technical and nontechnical management personnel who are designing or supporting the IT system. The questionnaire could also be used during on-site visits and interviews.

• **On-site Interviews.** Interviews with IT system support and management personnel can enable risk assessment personnel to collect useful information about the IT system (e.g., how the system is operated and managed). On-site visits also allow risk assessment personnel to observe and gather information about the physical, environmental, and operational security of the IT system. For systems still in the design phase, on-site visit would be face-to-face data gathering exercises and could provide the opportunity to evaluate the physical environment in which the IT system will operate.

• **Document Review.** Policy documents (e.g., legislative documentation, directives), system documentation (e.g., system user guide, system administrative manual, system

design and requirement document, acquisition document), and security-related documentation (e.g., previous audit report, risk assessment report, system test results, system security plan5, security policies) can provide good information about the security controls used by and planned for the IT system. An organization's mission impact analysis or asset criticality assessment provides information regarding system and data criticality and sensitivity.

• **Use of Automated Scanning Tool.** Proactive technical methods can be used to collect system information efficiently. For example, a network mapping tool can identify the services that run on a large group of hosts and provide a quick way of building individual profiles of the target IT system(s). Information gathering can be conducted throughout the risk assessment process, from Step 1 (System Characterization) through Step 9 (Results Documentation).

Output from Step 1- Characterization of the IT system assessed, a good picture of the IT system environment, and delineation of system boundary

STEP 2: THREAT IDENTIFICATION

A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. Vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised.

2.1 Threat-Source Identification

The goal of this step is to identify the potential threat-sources and compile a threat statement listing potential threat-sources that are applicable to the IT system being evaluated. A threat source is defined as any circumstance or event with the potential to cause harm to an IT system. The common threat sources can be natural, human, or environmental. In assessing threat-sources, it is important to consider all potential threat-sources that could cause harm to an IT system and its processing environment. For example, although the threat statement for an IT system located in a desert may not include "natural flood" because of the low likelihood of such an event occurring, environmental threats such as a bursting pipe can quickly flood a computer room and cause damage to an organization's IT assets and resources. Humans can be threat-sources through intentional acts, such as deliberate attacks by malicious persons or disgruntled employees, or unintentional acts, such as negligence and errors. A deliberate attack can be either (1) a malicious attempt to gain unauthorized access to an IT system (e.g., via password guessing) in order to compromise system and data integrity, availability, or confidentiality or (2) a benign, but nonetheless purposeful, attempt to circumvent system security. One example of the latter type of deliberate attack is a programmer's writing a Trojan horse program to bypass system security in order to "get the job done."

2.2 Motivation and Threat Actions

Motivation and the resources for carrying out an attack make humans potentially dangerous threat-sources. Table 1 presents an overview of many of today's common human threats, their possible motivations, and the methods or threat actions by which they might carry out an attack. This information will be useful to organizations studying their human threat environments and customizing their human threat statements. In addition, reviews of the history of system break-ins; security violation reports; incident reports; and interviews with the system administrators, help desk personnel, and user community during information gathering will help identify human threat-sources that have the potential to harm an IT system and its data and that may be a concern where vulnerability exists.

Table 1. Human Threats: Threat-Source, Motivation, and Threat Actions

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

An estimate of the motivation, resources, and capabilities that may be required to carry out a successful attack should be developed after the potential threat-sources have been

identified, in order to determine the likelihood of a threat's exercising a system vulnerability.

The threat statement, or the list of potential threat-sources, should be tailored to the individual organization and its processing environment (e.g., end-user computing habits). In general, information on natural threats (e.g., floods, earthquakes, storms) should be readily available.
Known threats have been identified by many government and private sector organizations.
Intrusion detection tools also are becoming more prevalent, and government and industry organizations continually collect data on security events, thereby improving the ability to realistically assess threats. Sources of information include, but are not limited to, the following:

1. Intelligence agencies (for example, the Federal Bureau of Investigation's National Infrastructure Protection Centre)
2. Federal Computer Incident Response Centre (FedCIRC)
3. Mass media, particularly Web-based resources such as SecurityFocus.com, SecurityWatch.com, SecurityPortal.com, and SANS.org.

Output from Step 2 - A threat statement containing a list of threat-sources that could exploit system vulnerabilities

STEP 3: VULNERABILITY IDENTIFICATION
The analysis of the threat to an IT system must include an analysis of the vulnerabilities associated with the system environment. The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources. Table 2 presents examples of vulnerability/threat pairs.

Table 2. Vulnerability/Threat Pairs

Vulnerability	Threat-Source	Threat Action
Terminated employees' system identifiers (ID) are not removed from the system	Terminated employees	Dialling into the company's network and accessing company proprietary data
Company firewall allows inbound telnet, and *guest* ID is enabled on XYZ server	Unauthorized users (e.g., hackers, terminated employees, computer criminals, terrorists)	Using telnet to XYZ server and browsing system files with the *guest* ID
The vendor has identified flaws in the security design	Unauthorized users (e.g., hackers, disgruntled	Obtaining unauthorized access to sensitive system

of the system; however, new patches have not been applied to the system	employees, computer criminals, terrorists)	files based on known system vulnerabilities
Data centre uses water sprinklers to suppress fire; tarpaulins to protect hardware and equipment from water damage are not in place	Fire, negligent persons	Water sprinklers being turned on in the data centre

Recommended methods for identifying system vulnerabilities are the use of vulnerability sources, the performance of system security testing, and the development of a security requirements checklist. It should be noted that the types of vulnerabilities that will exist, and the methodology needed to determine whether the vulnerabilities are present, will usually vary depending on the nature of the IT system and the phase it is in, in the SDLC:

• If the IT system has not yet been designed, the search for vulnerabilities should focus on the organization's security policies, planned security procedures, and system requirement definitions, and the vendors' or developers' security product analyses (e.g., white papers).

• If the IT system is being implemented, the identification of vulnerabilities should be expanded to include more specific information, such as the planned security features described in the security design documentation and the results of system certification test and evaluation.

• If the IT system is operational, the process of identifying vulnerabilities should include an analysis of the IT system security features and the security controls, technical and procedural, used to protect the system.

3.1 Vulnerability Sources

The technical and nontechnical vulnerabilities associated with an IT system's processing environment can be identified via the information-gathering techniques described in Section 1.2. A review of other industry sources (e.g., vendor Web pages that identify system bugs and flaws) will be useful in preparing for the interviews and in developing effective questionnaires to identify vulnerabilities that may be applicable to specific IT systems (e.g., a specific version of a specific operating system). The Internet is another source of information on known system vulnerabilities posted by vendors, along with hot fixes, service packs, patches, and other remedial measures that may be applied to eliminate or mitigate vulnerabilities. Documented vulnerability sources that should be considered in a thorough vulnerability analysis include, but are not limited to, the following:

• Previous risk assessment documentation of the IT system assessed

• The IT system's audit reports, system anomaly reports, security review reports, and system test and evaluation reports

• Vulnerability lists, such as the NIST I-CAT vulnerability database (http://icat.nist.gov)
• Security advisories, such as FedCIRC and the Department of Energy's Computer Incident Advisory Capability bulletins
• Vendor advisories
• Commercial computer incident/emergency response teams and post lists (e.g., SecurityFocus.com forum mailings)
• Information Assurance Vulnerability Alerts and bulletins for military systems
• System software security analyses.

3.2 System Security Testing

Proactive methods, employing system testing, can be used to identify system vulnerabilities efficiently, depending on the criticality of the IT system and available resources (e.g., allocated funds, available technology, persons with the expertise to conduct the test). Test methods include:

• Automated vulnerability scanning tool
• Security test and evaluation (ST&E)
• Penetration testing.

The automated vulnerability scanning tool is used to scan a group of hosts or a network for known vulnerable services (e.g., system allows anonymous File Transfer Protocol [FTP], sendmail relaying). However, it should be noted that some of the *potential* vulnerabilities identified by the automated scanning tool may not represent real vulnerabilities in the context of the system environment. For example, some of these scanning tools rate potential vulnerabilities without considering the site's environment and requirements. Some of the "vulnerabilities" flagged by the automated scanning software may actually not be vulnerable for a particular site but may be configured that way because their environment requires it. Thus, this test method may produce false positives. ST&E is another technique that can be used in identifying IT system vulnerabilities during the risk assessment process. It includes the development and execution of a test plan (e.g., test script, test procedures, and expected test results). The purpose of system security testing is to test the effectiveness of the security controls of an IT system as they have been applied in an operational environment. The objective is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standards. Penetration testing can be used to complement the review of security controls and ensure that different facets of the IT system are secured. Penetration testing, when employed in the risk assessment process, can be used to assess an IT system's ability to withstand intentional attempts to circumvent system security. Its objective is to test the IT system from the viewpoint of a threat-source and to identify potential failures in the IT system protection schemes. The results of these types of optional security testing will help identify a system's vulnerabilities.

3.3 Development of Security Requirements Checklist

During this step, the risk assessment personnel determine whether the security requirements stipulated for the IT system and collected during system characterization

are being met by existing or planned security controls. Typically, the system security requirements can be presented in table form, with each requirement accompanied by an explanation of how the system's design or implementation does or does not satisfy that security control requirement.

A security requirements checklist contains the basic security standards that can be used to systematically evaluate and identify the vulnerabilities of the assets (personnel, hardware, software, information), non-automated procedures, processes, and information transfers associated with a given IT system in the following security areas:

- Management
- Operational
- Technical.

Table 3 lists security criteria suggested for use in identifying an IT system's vulnerabilities in each security area.

Table 3. Security Criteria

Security Area	Security Criteria
Management Security	Assignment of responsibilities • Continuity of support • Incident response capability • Periodic review of security controls • Personnel clearance and background investigations • Risk assessment • Security and technical training • Separation of duties • System authorization and reauthorization • System or application security plan
Operational Security	• Control of air-borne contaminants (smoke, dust, chemicals) • Controls to ensure the quality of the electrical power supply • Data media access and disposal • External data distribution and labelling • Facility protection (e.g., computer room, data centre, office) • Humidity control • Temperature control • Workstations, laptops, and stand-alone personal computers
Technical Security	• Communications (e.g., dial-in, system interconnection, routers) • Cryptography • Discretionary access control • Identification and authentication • Intrusion detection • Object reuse • System audit

The outcome of this process is the security requirements checklist. Sources that can be used in compiling such a checklist include, but are not limited to, the following government regulatory and security directives and sources applicable to the IT system processing environment:

- CSA of 1987
- Federal Information Processing Standards Publications
- OMB November 2000 Circular A-130
- Privacy Act of 1974
- System security plan of the IT system assessed
- The organization's security policies, guidelines, and standards

• Industry practices.

The NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*, provides an extensive questionnaire containing specific control objectives against which a system or group of interconnected systems can be tested and measured. The control objectives are abstracted directly from long-standing requirements found in statute, policy, and guidance on security and privacy. The results of the checklist (or questionnaire) can be used as input for an evaluation of compliance and noncompliance. This process identifies system, process, and procedural weaknesses that represent potential vulnerabilities.

Output from Step 3 - A list of the system vulnerabilities (observations)7 that could be exercised by the potential threat-sources

STEP 4: CONTROL ANALYSIS

The goal of this step is to analyze the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability. To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment (Step 5 below), the implementation of current or planned controls must be considered. For example, a vulnerability (e.g., system or procedural weakness) is not likely to be exercised or the likelihood is low if there is a low level of threat-source interest or capability or if there are effective security controls that can eliminate, or reduce the magnitude of, harm. Sections 4.1 through 4.3, respectively, discuss control methods, control categories, and the control analysis technique.

4.1 Control Methods

Security controls encompass the use of technical and nontechnical methods. Technical controls are safeguards that are incorporated into computer hardware, software, or firmware (e.g., access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software). Nontechnical controls are management and operational controls, such as security policies; operational procedures; and personnel, physical, and environmental security.

4.2 Control Categories

The control categories for both technical and nontechnical control methods can be further classified as either preventive or detective. These two subcategories are explained as follows:

• Preventive controls inhibit attempts to violate security policy and include such controls as access control enforcement, encryption, and authentication.

• Detective controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums. The implementation of such controls during the risk mitigation process is the direct result of the identification of deficiencies in current or planned controls during the risk assessment process (e.g., controls are not in place or controls are not properly implemented).

4.3 Control Analysis Technique

As discussed in Section 3.3, development of a security requirements checklist or use of an available checklist will be helpful in analyzing controls in an efficient and systematic manner.

The security requirements checklist can be used to validate security noncompliance as well as compliance. Therefore, it is essential to update such checklists to reflect changes in an organization's control environment (e.g., changes in security policies, methods, and requirements) to ensure the checklist's validity.

Output from Step 4 - List of current or planned controls used for the IT system to mitigate the likelihood of a vulnerability's being exercised and reduce the impact of such an adverse event

STEP 5: LIKELIHOOD DETERMINATION

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered:

- Threat-source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls.

The likelihood that a potential vulnerability could be exercised by a given threat-source can be described as high, medium, or low. Table 4 below describes these three likelihood levels.

Table 4. Likelihood Definitions

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Output from Step 5 - Likelihood rating (High, Medium, Low)

STEP 6: IMPACT ANALYSIS

The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of a vulnerability. Before beginning the impact analysis, it is necessary to obtain the following necessary information as discussed in Section 3.

- System mission (e.g., the processes performed by the IT system)
- System and data criticality (e.g., the system's value or importance to an organization)
- System and data sensitivity.

This information can be obtained from existing organizational documentation, such as the mission impact analysis report or asset criticality assessment report. A mission impact analysis (also known as business impact analysis [BIA] for some organizations) prioritizes the impact levels associated with the compromise of an organization's information assets based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets. An asset criticality assessment identifies and prioritizes the sensitive and critical organization information assets (e.g., hardware, software, systems, services, and related technology assets) that support the organization's critical missions.

If this documentation does not exist or such assessments for the organization's IT assets have not been performed, the system and data sensitivity can be determined based on the level of protection required to maintain the system and data's availability, integrity, and confidentiality. Regardless of the method used to determine how sensitive an IT system and its data are, the system and information owners are the ones responsible for determining the impact level for their own system and information. Consequently, in analyzing impact, the appropriate approach is to interview the system and information owner(s). Therefore, the adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals: integrity, availability, and confidentiality. The following list provides a brief description of each security goal and the consequence (or impact) of its not being met:

• **Loss of Integrity.** System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.

• **Loss of Availability.** If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.

• **Loss of Confidentiality.** System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization. Some tangible impacts can be measured quantitatively in lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other impacts (e.g., loss of public confidence, loss of credibility, damage to an organization's interest) cannot be measured in specific units but

can be qualified or described in terms of high, medium, and low impacts. Because of the generic nature of this discussion, this guide designates and describes only the qualitative categories—high, medium, and low impact (see Table 5).

Table 5. Magnitude of Impact Definitions

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Quantitative versus Qualitative Assessment

In conducting the impact analysis, consideration should be given to the advantages and disadvantages of quantitative versus qualitative assessments. The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities. The disadvantage of the qualitative analysis is that it does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-benefit analysis of any recommended controls difficult. The major advantage of a quantitative impact analysis is that it provides a measurement of the impacts' magnitude, which can be used in the cost-benefit analysis of recommended controls. The disadvantage is that, depending on the numerical ranges used to express the measurement, the meaning of the quantitative impact analysis may be unclear, requiring the result to be interpreted in a qualitative manner. Additional factors often must be considered to determine the magnitude of impact. These may include, but are not limited to—

• An estimation of the frequency of the threat-source's exercise of the vulnerability over a specified time period (e.g., 1 year)

• An approximate cost for each occurrence of the threat-source's exercise of the vulnerability

• A weighted factor based on a subjective analysis of the relative impact of a specific threat's exercising a specific vulnerability.

Output from Step 6 - Magnitude of impact (High, Medium, or Low)

STEP 7: RISK DETERMINATION

The purpose of this step is to assess the level of risk to the IT system. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of:

• The likelihood of a given threat-source's attempting to exercise a given vulnerability

• The magnitude of the impact should a threat-source successfully exercise the vulnerability
• The adequacy of planned or existing security controls for reducing or eliminating risk.

To measure risk, a risk scale and a risk-level matrix must be developed. Section 7.1 presents a standard risk-level matrix; Section 7.2 describes the resulting risk levels.

7.1 Risk-Level Matrix

The final determination of mission risk is derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact. Table 6 below shows how the overall risk ratings might be determined based on inputs from the threat likelihood and threat impact categories. The matrix below is a 3 x 3 matrix of threat likelihood (High, Medium, and Low) and threat impact (High, Medium, and Low). Depending on the site's requirements and the granularity of risk assessment desired, some sites may use a 4 x 4 or a 5 x 5 matrix. The latter can include a Very Low /Very High threat likelihood and a Very Low/Very High threat impact to generate a Very Low/Very High risk level. A "Very High" risk level may require possible system shutdown or stopping of all IT system integration and testing efforts. The sample matrix in Table 6 shows how the overall risk levels of High, Medium, and Low are derived. The determination of these risk levels or ratings may be subjective. The rationale for this justification can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level. For example,
• The probability assigned for each threat likelihood level is 1.0 for High, 0.5 for Medium, 0.1 for Low
• The value assigned for each impact level is 100 for High, 50 for Medium, and 10 for Low.

Table 6. Risk-Level Matrix

Threat Likelihood	Impact		
	Low (10)	***Medium*** (50)	***High*** (100)
High (1.0)	**Low** 10 X 1.0 = 10	**Medium** 50 X 1.0 = 50	**High** 100 X 1.0 = 100
Medium (0.5)	**Low** 10 X 0.5 = 5	**Medium** 50 X 0.5 = 25	**Medium** 100 X 0.5 = 50
Low (0.1)	**Low** 10 X 0.1 = 1	**Low** 50 X 0.1 = 5	**Low** 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)

7.2 Description of Risk Level

Table 7 describes the risk levels shown in the above matrix. This risk scale, with its ratings of High, Medium, and Low, represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk scale also presents actions that senior management, the mission owners, must take for each risk level.

Table 7. Risk Scale and Necessary Actions

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.

Output from Step 7 - Risk level (High, Medium, Low)

STEP 8: CONTROL RECOMMENDATIONS

During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, are provided. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options (e.g., system compatibility)
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability.

The control recommendations are the results of the risk assessment process and provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented. It should be noted that not all possible recommended controls can be implemented to reduce loss. To determine which ones are required and appropriate for a specific organization, a cost-benefit analysis, as discussed in Section 4.6, should be conducted for the proposed recommended controls, to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. In addition, the operational impact (e.g.,

effect on system performance) and feasibility (e.g., technical requirements, user acceptance) of introducing the recommended option should be evaluated carefully during the risk mitigation process.

Output from Step 8-Recommendation of control(s) and alternative solutions to mitigate risk

STEP 9: RESULTS DOCUMENTATION

Once the risk assessment has been completed (threat-sources and vulnerabilities identified, risks assessed, and recommended controls provided), the results should be documented in an official report or briefing. A risk assessment report is a management report that helps senior management, the mission owners, make decisions on policy, procedural, budget, and system operational and management changes. Unlike an audit or investigation report, which looks for wrongdoing, a risk assessment report should not be presented in an accusatory manner but as a systematic and analytical approach to assessing risk so that senior management will understand the risks and allocate resources to reduce and correct potential losses. For this reason, some people prefer to address the threat/vulnerability pairs as observations instead of findings in the risk assessment report.

Output from Step 9 - Risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation

Self Assessment Exercise

1. What do you understand by these terms?
   a. vulnerability,
   b. Threat Source and
   c. Threat action
   d. Risk-Level Matrix

4.0 Conclusion

Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization. Having discussed the several steps involved in assessing risk in any IT system, it becomes clearer that the adverse effect of immediate and future risk cannot be overemphasised be it at the level of input or output in information management.

5.0 Summary

This unit examines risk assessment with particular emphasis on methodology which encompasses nine primary steps: System Characterization, Threat Identification, Vulnerability Identification, Control Analysis, Likelihood Determination, Impact

Analysis, Risk Determination, Control Recommendations, and Results Documentation. However these steps are no Straight-jackets rules, it could take several other patterns.

6.0 Tutor Marked Assignment

a. What is a Threat-Source?
b. How do you go about the Identification of a threat-source?

7.0 References/Further Reading

Computer Systems Laboratory Bulletin. *Threats to Computer Systems: An Overview*. March 1994.

NIST Interagency Reports 4749. *Sample Statements of Work for Federal Computer Security*
Services: For Use In-House or Contracting Out. December 1991.

NIST Special Publication 800-12. *An Introduction to Computer Security: The NIST Handbook*. October 1995.

NIST Special Publication 800-14. *Generally Accepted Principles and Practices for Securing*
Information Technology Systems. September 1996. Co-authored with Barbara Guttman.

NIST Special Publication 800-18. *Guide For Developing Security Plans for Information Technology Systems*. December 1998. Co-authored with Federal Computer Security Managers' Forum Working Group.

NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*. August 2001.

NIST Special Publication 800-27. *Engineering Principles for IT Security*. June 2001.
OMB Circular A-130. *Management of Federal Information Resources.* Appendix III. November 2000.

UNIT 4
RISK MITIGATION OPTIONS

Content

1.0 Introduction

Risk mitigation, the second process of risk management, involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior management and functional and business managers to use the *least-cost approach* and implement the *most appropriate controls* to decrease mission risk to an acceptable level, with *minimal adverse impact* on the organization's resources and mission.

2.0 Objectives

Students are expected to know:

1. the various risk mitigation options and strategy.
2. the approaches for risk mitigation control, implementation and control categories,
3. the cost-benefit analysis in risk control.

3.0 Main body

Risk mitigation is a systematic methodology used by senior management to reduce mission risk. Risk mitigation can be achieved through any of the following options.

1. Risk Mitigation Options:

• **Risk Assumption.** To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level
• **Risk Avoidance.** To avoid the risk by eliminating the risk cause and/or consequence (e.g., forego certain functions of the system or shut down the system when risks are identified)
• **Risk Limitation.** To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls)

• **Risk Planning.** To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls
• **Research and Acknowledgment.** To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability
• **Risk Transference.** To transfer the risk by using other options to compensate for the loss, such as purchasing insurance. The goals and mission of an organization should be considered in selecting any of these risk mitigation options. It may not be practical to address all identified risks, so priority should be given to the threat and vulnerability pairs that have the potential to cause significant mission impact or harm. Also, in safeguarding an organization's mission and its IT systems, because of each organization's unique environment and objectives, the option used to mitigate the risk and the methods used to implement controls may vary. The "best of breed" approach is to use appropriate technologies from among the various vendor security products, along with the appropriate risk mitigation option and nontechnical, administrative measures.

2. RISK MITIGATION STRATEGY

Senior management, the mission owners, knowing the potential risks and recommended controls, may ask, "When and under what circumstances should I take action? When shall I implement these controls to mitigate the risk and protect our organization?"
The risk mitigation chart in Figure 1 addresses these questions. Appropriate points for implementation of control actions are indicated in this figure by the word YES.

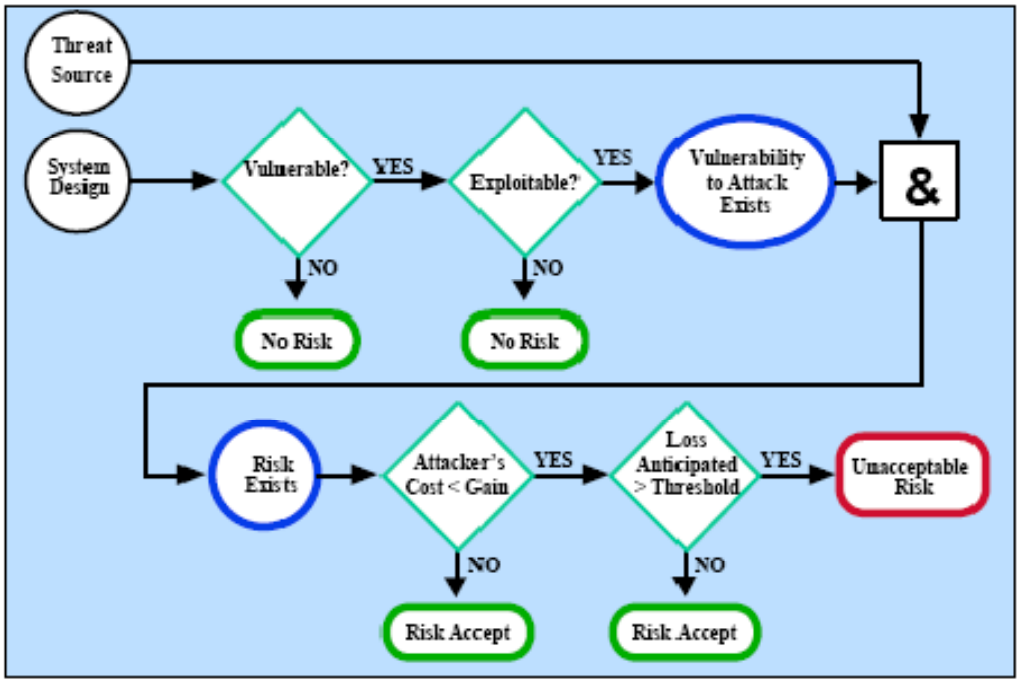


Figure 1. Risk Mitigation Action Points

This strategy is further articulated in the following rules of thumb, which provide guidance on actions to mitigate risks from intentional human threats:

• **When vulnerability (or flaw, weakness) exists →** implement assurance techniques to reduce the likelihood of a vulnerability's being exercised.
• **When vulnerability can be exercised →** apply layered protections, architectural designs, and administrative controls to minimize the risk of or prevent this occurrence.
• **When the attacker's cost is less than the potential gain →** apply protections to decrease an attacker's motivation by increasing the attacker's cost (e.g., use of system controls such as limiting what a system user can access and do can significantly reduce an attacker's gain).
• **When loss is too great →** apply design principles, architectural designs, and technical and nontechnical protections to limit the extent of the attack, thereby reducing the potential for loss. The strategy outlined above, with the exception of the third list item ("When the attacker's cost is less than the potential gain"), also applies to the mitigation of risks arising from environmental or unintentional human threats (e.g., system or user errors). (Because there is no "attacker," no motivation or gain is involved.).

3 APPROACHES FOR CONTROL IMPLEMENTATION

When control actions must be taken, the following rules apply:

Address the greatest risks and strive for sufficient risk mitigation at the lowest cost, with minimal impact on other mission capabilities.

The following risk mitigation methodology describes the approach to control implementation:

• Step 1-Prioritize Actions

Based on the risk levels presented in the risk assessment report, the implementation actions are prioritized. In allocating resources, top priority should be given to risk items with unacceptably high risk rankings (e.g., risk assigned a Very High or High risk level). These vulnerability/threat pairs will require immediate corrective action to protect an organization's interest and mission.

Output from Step 1-Actions ranking from High to Low

• Step 2-Evaluate Recommended Control Options

The controls recommended in the risk assessment process may not be the most appropriate and feasible options for a specific organization and IT system. During this step, the feasibility (e.g., compatibility, user acceptance) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended control options are analyzed. The objective is to select the most appropriate control option for minimizing risk.

Output from Step 2-List of feasible controls

• Step 3-Conduct Cost-Benefit Analysis

To aid management in decision making and to identify cost-effective controls, a cost-benefit analysis is conducted. Section.5 details the objectives and method of conducting the cost-benefit analysis.

Output from Step 3-Cost-benefit analysis describing the cost and benefits of implementing or not implementing the controls

• Step 4-Select Control

On the basis of the results of the cost-benefit analysis, management determines the most cost-effective control(s) for reducing risk to the organization's mission. The controls selected should combine technical, operational, and management control elements to ensure adequate security for the IT system and the organization.

Output from Step 4 Selected control(s)

• Step 5-Assign Responsibility

Appropriate persons (in-house personnel or external contracting staff) who have the appropriate expertise and skill-sets to implement the selected control are identified, and responsibility is assigned.

Output from Step 5-List of responsible persons

• Step 6-Develop a Safeguard Implementation Plan

During this step, a safeguard implementation plan (or action plan) is developed. The plan should, at a minimum, contain the following information:

– Risks (vulnerability/threat pairs) and associated risk levels (output from risk assessment report)
– Recommended controls (output from risk assessment report)
– Prioritized actions (with priority given to items with Very High and High risk levels)
– Selected planned controls (determined on the basis of feasibility, effectiveness, benefits to the organization, and cost)
– Required resources for implementing the selected planned controls
– Lists of responsible teams and staff
– Start date for implementation
– Target completion date for implementation
– Maintenance requirements.

The safeguard implementation plan prioritizes the implementation actions and projects the start and target completion dates. This plan will aid and expedite the risk mitigation process. Appendix C provides a sample summary table for the safeguard implementation plan.

Output from Step 6-Safeguard implementation plan

• Step 7-Implement Selected Control(s)

Depending on individual situations, the implemented controls may lower the risk level but not eliminate the risk. Residual risk is discussed in Section 4.6.

Output from Step 7-Residual risk

Figure 4-2 depicts the recommended methodology for risk mitigation.

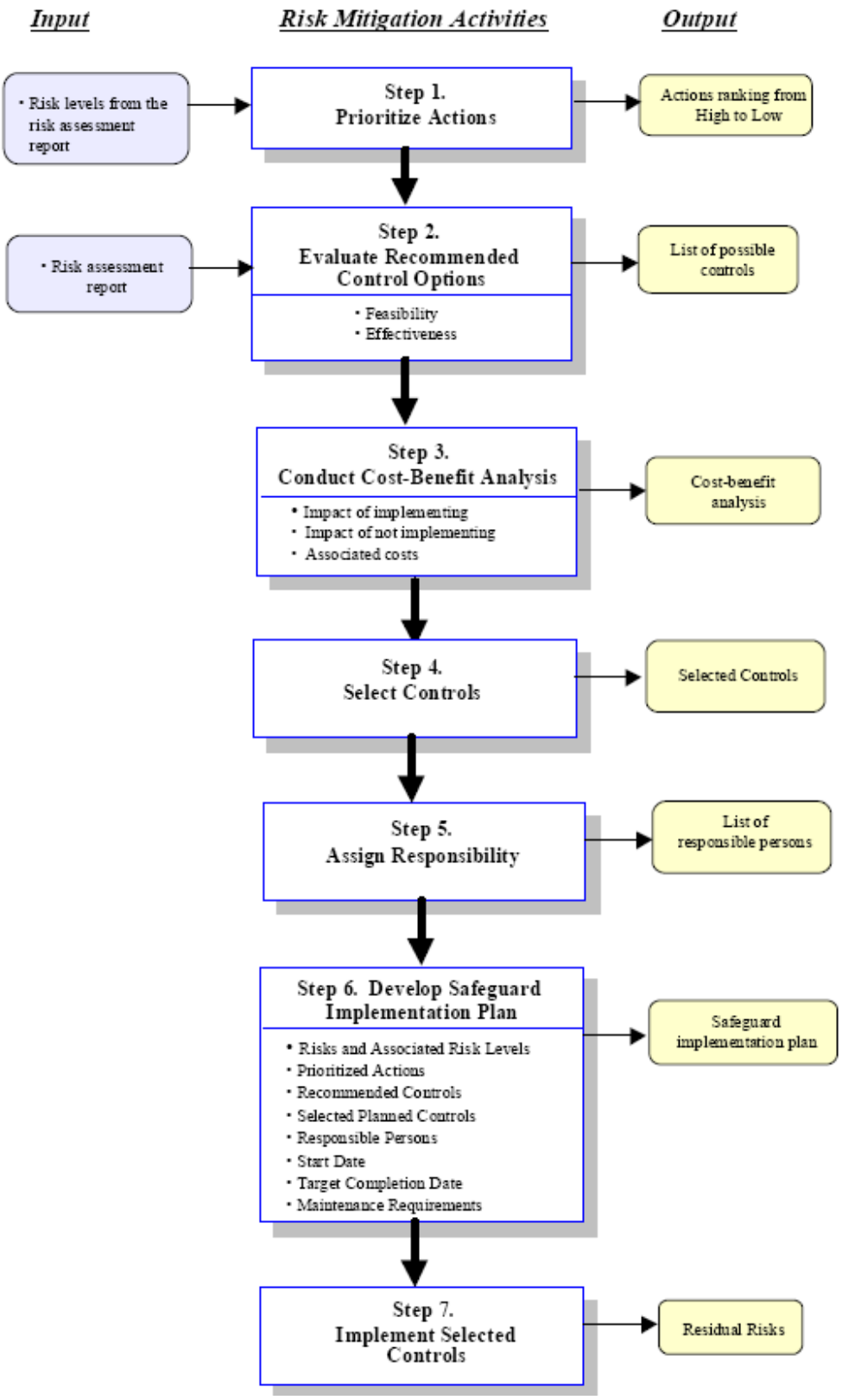


Figure 2. Risk Mitigation Methodology Flowchart

4 CONTROL CATEGORIES

In implementing recommended controls to mitigate risk, an organization should consider technical, management, and operational security controls, or a combination of such controls, to maximize the effectiveness of controls for their IT systems and organization. Security controls, when used appropriately, can prevent, limit, or deter threat-source damage to an organization's mission. The control recommendation process will involve choosing among a combination of technical, management, and operational controls for improving the organization's security posture. The trade-offs that an organization will have to consider are illustrated by viewing the decisions involved in enforcing use of complex user passwords to minimize password guessing and cracking. In this case, a technical control requiring add-on security software may be more complex and expensive than a procedural control, but the technical control is likely to be more effective because the enforcement is automated by the system. On the other hand, a procedural control might be implemented simply by means of a memorandum to all concerned individuals and an amendment to the security guidelines for the organization, but ensuring that users consistently follow the memorandum and guideline will be difficult and will require security awareness training and user acceptance. This section provides a high-level overview of some of the control categories. Sections 4.1 through 4.3 provide an overview of technical, management, and operational controls, respectively.

4.1 Technical Security Controls

Technical security controls for risk mitigation can be configured to protect against given types of threats. These controls may range from simple to complex measures and usually involve system architectures; engineering disciplines; and security packages with a mix of hardware, software, and firmware. All of these measures should work together to secure critical and sensitive data, information, and IT system functions. Technical controls can be grouped into the following major categories, according to primary purpose:

- **Support** (Section 4.1.1). Supporting controls are generic and underlie most IT security capabilities. These controls must be in place in order to implement other controls.
- **Prevent** (Section 4.1.2). Preventive controls focus on preventing security breaches from occurring in the first place.
- **Detect and Recover** (Section 4.1.3). These controls focus on detecting and recovering from a security breach.

Figure 3 depicts the primary technical controls and the relationships between them.

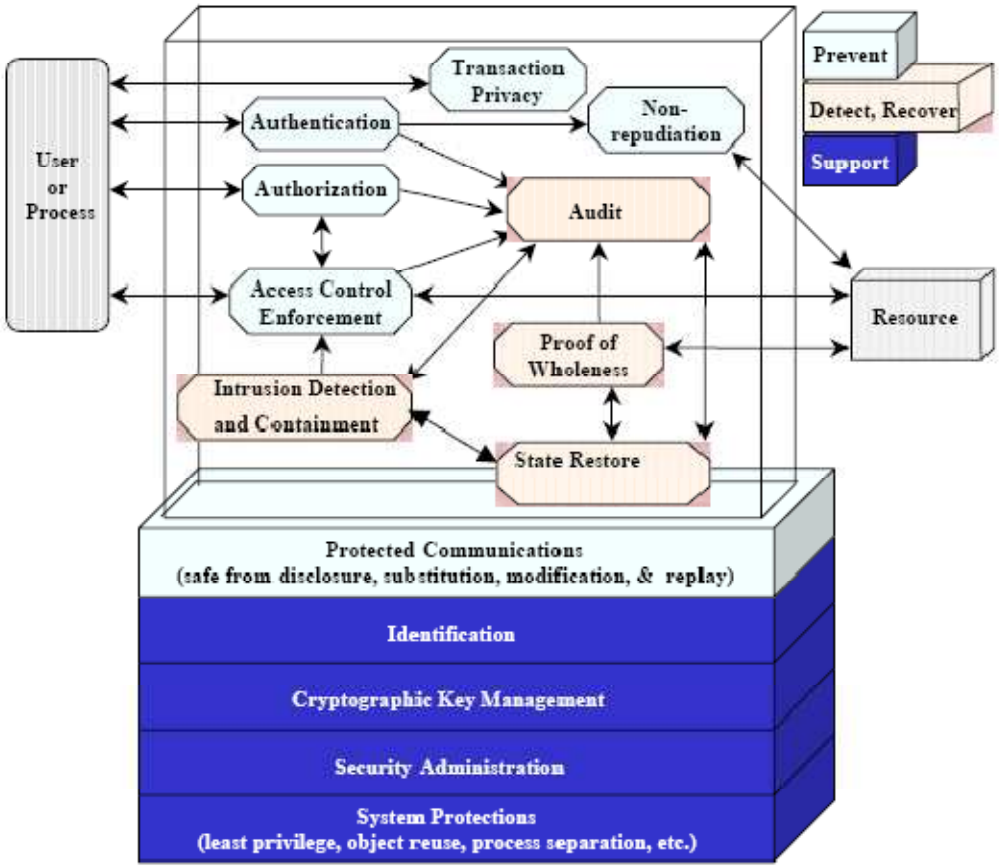


Figure 3. Technical Security Controls

4.1.1 *Supporting Technical Controls*

Supporting controls are, by their very nature, pervasive and interrelated with many other controls. The supporting controls are as follows:

• **Identification.** This control provides the ability to uniquely identify users, processes, and information resources. To implement other security controls (e.g., discretionary access control [DAC], mandatory access control [MAC], accountability), it is essential that both subjects and objects be identifiable.

• **Cryptographic Key Management.** Cryptographic keys must be securely managed when cryptographic functions are implemented in various other controls. Cryptographic key management includes key generation, distribution, storage, and maintenance.

• **Security Administration.** The security features of an IT system must be configured (e.g., enabled or disabled) to meet the needs of a specific installation and to account for changes in the operational environment. System security can be built into operating system security or the application. Commercial off-the-shelf add-on security products are available.

• **System Protections.** Underlying a system's various security functional capabilities is a base of confidence in the technical implementation. This represents the quality of the implementation from the perspective both of the design processes used and of the manner in which the implementation was accomplished. Some examples of system protections are residual information protection (also known as object reuse), least privilege (or "need to know"), process separation, modularity, layering, and minimization of what needs to be trusted.

4.1.2 *Preventive Technical Controls*

These controls, which can inhibit attempts to violate security policy, include the following:

• **Authentication.** The authentication control provides the means of verifying the identity of a subject to ensure that a claimed identity is valid. Authentication mechanisms include passwords, personal identification numbers, or PINs, and emerging authentication technology that provides strong authentication (e.g., token, smart card, digital certificate, Kerberos).

• **Authorization.** The authorization control enables specification and subsequent management of the allowed actions for a given system (e.g., the information owner or the database administrator determines who can update a shared file accessed by a group of online users).

• **Access Control Enforcement.** Data integrity and confidentiality are enforced by access controls. When the subject requesting access has been authorized to access particular processes, it is necessary to enforce the defined security policy (e.g., MAC or DAC). These policy-based controls are enforced via access control mechanisms distributed throughout the system (e.g., MAC sensitivity labels; DAC file permission sets, access control lists, roles, user profiles). The effectiveness and the strength of access control depend on the correctness of the access control decisions (e.g., how the security rules are configured) and the strength of access control enforcement (e.g., the design of software or hardware security).

• **Nonrepudiation.** System accountability depends on the ability to ensure that senders cannot deny sending information and that receivers cannot deny receiving it. Nonrepudiation spans both prevention and detection. It has been placed in the prevention category in this guide because the mechanisms implemented prevent the successful repudiation of an action (e.g., the digital certificate that contains the owner's private key is known only to the owner). As a result, this control is typically applied at the point of transmission or reception.

• **Protected Communications.** In a distributed system, the ability to accomplish security objectives is highly dependent on trustworthy communications. The protected communications control ensures the integrity, availability, and confidentiality of sensitive and critical information while it is in transit. Protected communications use data encryption methods (e.g., virtual private network, Internet Protocol Security [IPSEC] Protocol), and deployment of cryptographic technologies (e.g., Data Encryption Standard [DES], Triple DES, RAS, MD4, MD5, secure hash standard, and escrowed encryption

algorithms such as Clipper) to minimize network threats such as replay, interception, packet sniffing, wiretapping, or eavesdropping.

• **Transaction Privacy.** Both government and private sector systems are increasingly required to maintain the privacy of individuals. Transaction privacy controls (e.g., Secure Sockets Layer, secure shell) protect against loss of privacy with respect to transactions performed by an individual.

4.1.3 *Detection and Recovery Technical Controls*

Detection controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums. Recovery controls can be used to restore lost computing resources. They are needed as a complement to the supporting and preventive technical measures, because none of the measures in these other areas is perfect.

Detection and recovery controls include—

• **Audit.** The auditing of security-relevant events and the monitoring and tracking of system abnormalities are key elements in the after-the-fact detection of, and recovery from, security breaches.

• **Intrusion Detection and Containment.** It is essential to detect security breaches (e.g., network break-ins, suspicious activities) so that a response can occur in a timely manner. It is also of little use to detect a security breach if no effective response can be initiated. The intrusion detection and containment control provides these two capabilities.

• **Proof of Wholeness.** The proof-of-wholeness control (e.g., system integrity tool) analyzes system integrity and irregularities and identifies exposures and potential threats. This control does not prevent violations of security policy but detects violations and helps determine the type of corrective action needed.

• **Restore Secure State.** This service enables a system to return to a state that is known to be secure, after a security breach occurs.

• **Virus Detection and Eradication.** Virus detection and eradication software installed on servers and user workstations detects, identifies, and removes software viruses to ensure system and data integrity.

4.2 Management Security Controls

Management security controls, in conjunction with technical and operational controls, are implemented to manage and reduce the risk of loss and to protect an organization's mission. Management controls focus on the stipulation of information protection policy, guidelines, and standards, which are carried out through operational procedures to fulfill the organization's goals and missions. Management security controls—preventive, detection, and recovery—that are implemented to reduce risk are described in Sections4.2.1 through 4.2.3.

4.2.1 Preventive Management Security Controls

These controls include the following:

• Assign security responsibility to ensure that adequate security is provided for the mission-critical IT systems

• Develop and maintain system security plans to document current controls and address planned controls for IT systems in support of the organization's mission
• Implement personnel security controls, including separation of duties, least privilege, and user computer access registration and termination
• Conduct security awareness and technical training to ensure that end users and system users are aware of the rules of behaviour and their responsibilities in protecting the organization's mission.

4.2.2 Detection Management Security Controls

Detection management controls are as follows:
• Implement personnel security controls, including personnel clearance, background investigations, rotation of duties
• Conduct periodic review of security controls to ensure that the controls are effective
• Perform periodic system audits
• Conduct ongoing risk management to assess and mitigate risk
• Authorize IT systems to address and accept residual risk.

4.2.3 Recovery Management Security Controls

These controls include the following:
• Provide continuity of support and develop, test, and maintain the continuity of operations plan to provide for business resumption and ensure continuity of operations during emergencies or disasters
• Establish an incident response capability to prepare for, recognize, report, and respond to the incident and return the IT system to operational status.

4.3 Operational Security Controls

An organization's security standards should establish a set of controls and guidelines to ensure that security procedures governing the use of the organization's IT assets and resources are properly enforced and implemented in accordance with the organization's goals and mission. Management plays a vital role in overseeing policy implementation and in ensuring the establishment of appropriate operational controls. Operational controls, implemented in accordance with a base set of requirements (e.g., technical controls) and good industry practices, are used to correct operational deficiencies that could be exercised by potential threat-sources. To ensure consistency and uniformity in security operations, step-by-step procedures and methods for implementing operational controls must be clearly defined, documented, and maintained. These operational controls include those presented in Sections 4.3.1 and 4.3.2 below.

4.3.1 Preventive Operational Controls

Preventive operational controls are as follows:
• Control data media access and disposal (e.g., physical access control, degaussing method)

• Limit external data distribution (e.g., use of labelling)
• Control software viruses
• Safeguard computing facility (e.g., security guards, site procedures for visitors, electronic badge system, biometrics access control, management and distribution of locks and keys, barriers and fences)
• Secure wiring closets that house hubs and cables
• Provide backup capability (e.g., procedures for regular data and system backups, archive logs that save all database changes to be used in various recovery scenarios)
• Establish off-site storage procedures and security
• Protect laptops, personal computers (PC), workstations
• Protect IT assets from fire damage (e.g., requirements and procedures for the use of fire extinguishers, tarpaulins, dry sprinkler systems, halon fire suppression system)
• Provide emergency power source (e.g., requirements for uninterruptible power supplies, on site power generators)
• Control the humidity and temperature of the computing facility (e.g., operation of air conditioners, heat dispersal).

4.3.2 Detection Operational Controls

Detection operational controls include the following:
• Provide physical security (e.g., use of motion detectors, closed-circuit television monitoring, sensors and alarms)
• Ensure environmental security (e.g., use of smoke and fire detectors, sensors and alarms).

5 COST-BENEFIT ANALYSIS

To allocate resources and implement cost-effective controls, organizations, after identifying all possible controls and evaluating their feasibility and effectiveness, should conduct a cost-benefit analysis for each proposed control to determine which controls are required and appropriate for their circumstances. The cost-benefit analysis can be qualitative or quantitative. Its purpose is to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. For example, the organization may not want to spend ₦1,000 on a control to reduce a ₦200 risk. A cost-benefit analysis for proposed new controls or enhanced controls encompasses the following:
• Determining the impact of implementing the new or enhanced controls
• Determining the impact of *not* implementing the new or enhanced controls
• Estimating the costs of the implementation. These may include, but are not limited to, the following:
– Hardware and software purchases
– Reduced operational effectiveness if system performance or functionality is reduced for increased security
– Cost of implementing additional policies and procedures

– Cost of hiring additional personnel to implement proposed policies, procedures, or services
– Training costs
– Maintenance costs
• Assessing the implementation costs and benefits against system and data criticality to determine the importance to the organization of implementing the new controls, given their costs and relative impact. The organization will need to assess the benefits of the controls in terms of maintaining an acceptable mission posture for the organization. Just as there is a cost for implementing a needed control, there is a cost for not implementing it. By relating the result of not implementing the control to the mission, organizations can determine whether it is feasible to forego its implementation.

Cost-Benefit Analysis Example: System X stores and processes mission-critical and sensitive employee privacy information; however, auditing has not been enabled for the system. A cost-benefit analysis is conducted to determine whether the audit feature should be enabled for System X. Items (1) and (2) address the intangible impact (e.g., deterrence factors) for implementing or not implementing the new control. Item (3) lists the tangibles (e.g., actual cost).
(1) Impact of enabling system audit feature: The system audit feature allows the system security administrator to monitor users' system activities but will slow down system performance and therefore affect user productivity. Also the implementation will require additional resources, as described in Item 3.

(2) Impact of not enabling system audit feature: User system activities and violations cannot be monitored and tracked if the system audit function is disabled, and security cannot be maximized to protect the organization's confidential data and mission.
(3) Cost estimation for enabling the system audit feature:

Cost for enabling system audit feature—No cost, built-in feature	₦ 0
Additional staff to perform audit review and archive, per year	₦ XX,XXX
Training (e.g., system audit configuration, report generation)	₦ X,XXX
Add-on audit reporting software	₦ X,XXX
Audit data maintenance (e.g., storage, archiving), per year	₦ X,XXX
Total Estimated Costs	**₦ XX,XXX**

The organization's managers must determine what constitutes an acceptable level of mission risk. The impact of a control may then be assessed, and the control either included or excluded, after the organization determines a range of feasible risk levels. This range will vary among organizations; however, the following rules apply in determining the use of new controls:

• If control would reduce risk more than needed, then see whether a less expensive alternative exists

• If control would cost more than the risk reduction provided, then find something else

• If control does not reduce risk sufficiently, then look for more controls or a different control

• If control provides enough risk reduction and is cost-effective, then use it.

Frequently the cost of implementing a control is more tangible than the cost of not implementing it. As a result, senior management plays a critical role in decisions concerning the implementation of control measures to protect the organizational mission.

6 RESIDUAL RISKS

Organizations can analyze the extent of the risk reduction generated by the new or enhanced controls in terms of the reduced threat likelihood or impact, the two parameters that define the mitigated level of risk to the organizational mission.

Implementation of new or enhanced controls can mitigate risk by-

• Eliminating some of the system's vulnerabilities (flaws and weakness), thereby reducing the number of possible threat-source/vulnerability pairs

• Adding a targeted control to reduce the capacity and motivation of a threat-source

For example, a department determines that the cost for installing and maintaining add-on security software for the stand-alone PC that stores its sensitive files is not justifiable, but that administrative and physical controls should be implemented to make physical access to that PC more difficult (e.g., store the PC in a locked room, with the key kept by the manager).

• Reducing the magnitude of the adverse impact (for example, limiting the extent of a vulnerability or modifying the nature of the relationship between the IT system and the organization's mission).

The relationship between control implementation and residual risk is graphically presented in Figure 4 below.

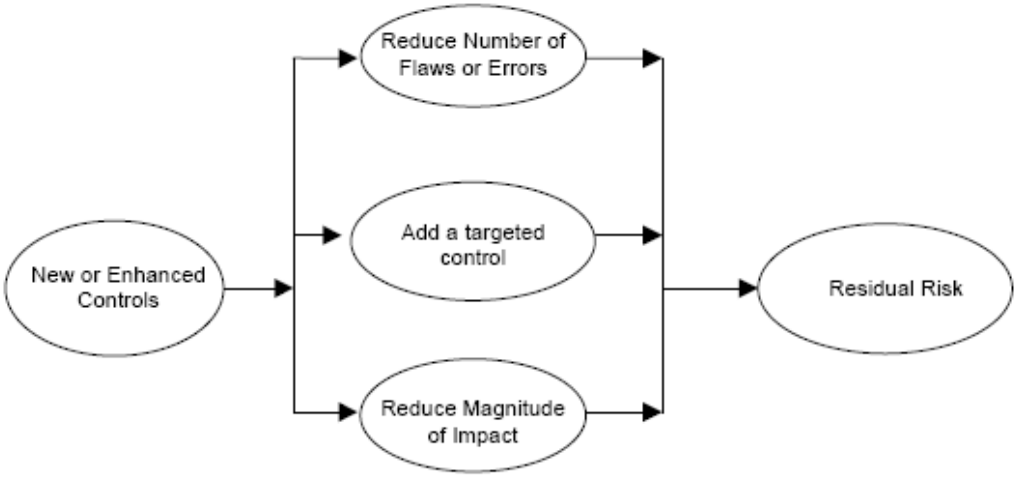


Figure 4. Implemented Controls and Residual Risk

The risk remaining after the implementation of new or enhanced controls is the residual risk. Practically no IT system is risk free, and not all implemented controls can eliminate the risk they are intended to address or reduce the risk level to zero. The intent of this process is to identify risks that are not fully addressed and to determine whether additional controls are needed to mitigate the risks identified in the IT system.

Self Assessment Exercise

1. List and explain the six risk mitigation options.
2. What is supporting and preventive control in risk mitigation options?

4.0 Conclusion

In most organizations, the network itself will continually be expanded and updated, its components changed, and its software applications replaced or updated with newer versions. In addition, personnel changes will occur and security policies are likely to change over time.

These changes mean that new risks will surface and risks previously mitigated may again become a concern. Thus, the risk management process is ongoing and evolving. There should be a specific schedule for assessing and mitigating mission risks, but the periodically performed process should also be flexible enough to allow changes where warranted, such as major changes to the IT system and processing environment due to changes resulting from policies and new technologies. A successful risk management program will rely on management's commitment; (2) the full support and participation of the IT team (3) the competence of the risk assessment team, which must have the expertise to apply the risk assessment methodology to a specific site and system, identify mission risks, and provide cost-effective safeguards that meet the needs of the organization; (4) the awareness and cooperation of members of the user community, who

must follow procedures and comply with the implemented controls to safeguard the mission of their organization; and (5) an ongoing evaluation and assessment of the IT-related mission risks.

5.0 Summary

This unit describes risk mitigation options (Section 1), the risk mitigation strategy (Section 2), an approach for control implementation (Section 3), control categories (Section 4), the cost-benefit analysis used to justify the implementation of the recommended controls (Section 5), and residual risk (Section 6).

6.0 Tutor Marked Assignment

Draw a Risk Mitigation Methodology Flowchart and explain how it works.

7.0 References/Further Reading

Computer Systems Laboratory Bulletin. *Threats to Computer Systems: An Overview*. March 1994.

NIST Interagency Reports 4749. *Sample Statements of Work for Federal Computer Security*
Services: For Use In-House or Contracting Out. December 1991.

NIST Special Publication 800-12. *An Introduction to Computer Security: The NIST Handbook*. October 1995.

NIST Special Publication 800-14. *Generally Accepted Principles and Practices for Securing*
Information Technology Systems. September 1996. Co-authored with Barbara Guttman.

NIST Special Publication 800-18. *Guide For Developing Security Plans for Information Technology Systems*. December 1998. Co-authored with Federal Computer Security Managers' Forum Working Group.

NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*. August 2001.

NIST Special Publication 800-27. *Engineering Principles for IT Security*. June 2001.
OMB Circular A-130. *Management of Federal Information Resources.* Appendix III. November 2000.

UNIT 5

Mitigating Economic Risk Through Security Technology

Content

1.0 Introduction

Appearing daily across the headlines of major newspapers and periodicals, global security has moved to the forefront on business concern. And the economic losses ascribed to such attacks and breaches totals a staggering sum in billions of dollars (US) annually for companies spanning the continents. For businesses of electronic commerce and highly concentrated information architectures, these disruption figures soar even higher than traditional manufacturing and service sectors.

2.0 Objectives

This unit defines the components of risk mitigation through the investment in firewall appliances and server-side preservation technologies. Students are expected to know some descriptive statistics that illuminate real-world occurrences, the numerical values contained herein and how they can be applied in every organization.

3.0 Main body

Risk begins with a perceived vulnerability and the acceptance of safeguard methods to reduce the likelihood of a negative or undesired outcome. In the economic sense, risk is largely concerned with probability of such adverse outcomes and what factors contribute positively to produce such an event. To an IT manager, risk might mean the chance or frequency of disruption in the network environment—intentionally or unintentionally. Still, the subject of risk cannot be ignored from a contingency planning or information asset point of view. Staying within the purview of the IT and network realm, risk imparts a need for attention in three distinct areas: *definition*, *measurement* and *mitigation*. *Definition* of risk precedes any other component because it starts with setting boundaries—or zones—that determine the scope and outcome of any undesired outcome. For instance, not having a firewall in place for your Internet gateway allows free roaming of public users within the four walls of your business. Risk inviting? Absolutely. A host

of undesirable outcomes can unfold and inflict significant harm among your employees and their productivity. But what about setting scope and boundaries? Internet access may only be limited to a specific server, or external gateway, in which case damage is restricted to a concise section of your IT environment. Limits—and the ability to define zones of impact—are of primary importance in the process of defining risk and its total impact on the organization. These limits, with regard to network operations, have been analyzed and studied as linear functions to ascertain different types of exposure and their relative probability of negative outcome. In other words, setting limits on the type of user (e.g. wired network versus wireless) can allow us to set the boundaries for assigning criteria to the risk equation. While most things can be measured, few tasks are more difficult than establishing the actual definition of risk as an inventory of impacted resources and outcome probabilities.

Next, with our definition of risk in hand, we move to understand how to *measure* risk itself. Since risk is comprised of negative outcomes and their assigned probabilities, it is best to start the measurement process by taking an inventory of the various types of outcome that may occur and with what frequency they can be observed. During the course of studying a wide breadth of organizations and their network operations, several dominant risk outcomes clustered themselves in the following categories:

a) **Internal Disruption**—the compromise of network assets as a result of unauthorized or intentional intrusion from a firm's employee or validated user

b) **Passive Code-Level Intrusion**—the introduction of software agents or script code to the network environment (e.g. worms, viruses, etc.)

c) **External Disruption**—the intentional and manual process of network or information disruption by an outside system or individual (e.g. network hackers, denial of service interruption, etc.)

d) **Authentication Forgery**—the use of forged identity credentials to gain access to information assets or systems without authorization

e) **Extraction**—the intentional or unintentional export or deletion of information assets without authorization

Looking at each of these risk categories, we can look at the data and make two additional determinations regarding frequency (as a probability) and the extent of each in terms of damage (magnitude of loss). In Figure 1.1, a list of these categories is given alongside the corresponding range of frequencies and the measured average value of loss (in whole US dollars) associated with these activities. Keeping in mind that these data were collected across organizations of disparate sizes (from small businesses to large enterprises), the order of scale in terms of frequency and size of loss for your particular

organization may be higher or lower, depending upon several key factors. In our assessment of these elements affecting network vulnerability, we applied statistical patterns produced by Factor Analysis to determine positive correlation among the following variables:

a) **Employee Density**—the number of employees within an organization

b) **Branch Locations**—the number of branch facilities of locations outside of the parent headquarters

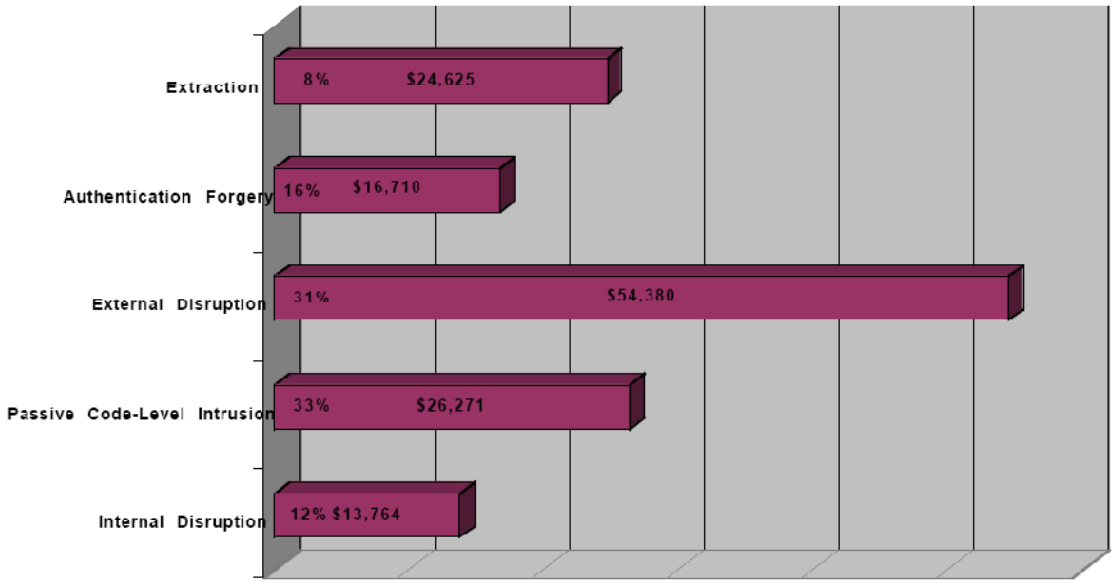
c) **Type of Operations**—the primary nature of business products and services, ranging from the production of low-skilled consumer goods to complex intellectual services

d) **Employee Mobility**—the ability and capacity for employees to access network services outside of a wired LAN environment)

e) **Average Employee Earnings**—the threshold dollar amounts paid to employees as compensation for labor earnings

f) **Annual Gross Revenue Product (AGRP)**—the amount, adjusted in US dollars, of an organization's earnings or intake of capital proceeds

Figure 1.1 Dominant Risk Outcomes
Shown here with relative percentage of frequency and average loss value per incident



Economists and statisticians alike use the method of Factor Analysis to boil down the most important variables of any measurement equation so as to assess their interaction with each other and determine relationships. For network security purposes, the above-

listed variables proved to be the key factors associated with risk of loss and measuring the loss proportions in differing organizations. It is important to remember that the frequency of loss varies according to the relative change of other variables, and likewise the magnitude changes according to the same. The end game, however, is wrapped inside the *mitigation* process and how we abate risk by lowering our odds of such predictable negative outcomes. Traditional insurance companies, and even those insuring losses in the digital property space, rely upon actuarial figures and statistics to determine a premium for an insurance policy—to hedge against the risk of loss based upon known criterion. In computing the premium, the information regarding the policyholder's risk environment is scored and then aligned to a premium rate structure. Again, based on known factors such as those in Figure 1.1, we can begin to look at technologies that lower our risk of exposure to malicious attacks and disruption of information assets—forcing a significant reduction in the probability of facing such negative circumstances. And by analyzing your organization's risk position in contrast to its relative bearing for loss, the value proposition becomes one of economic sensibility in exchange of money spent for mitigation of risk associated with the undesired effects.

Technology Contrast: A Case for Economic Investment

A number of firewall technology vendors produce solutions focused upon protecting individual users and the IT environment at large from the thwart of hacker penetration and malicious attack—risks that ultimately disrupt business operations and impose considerable costs of recovery. In looking at any technology offering as a composite of risk mitigation and network enhancement benefits, the referendum for an investment decision is one that goes much deeper than a simple ROI (return on investment) calculation—rather it supports a wide value chain. And to get a firm grasp on these value chain constituents, an economic method or theory known as Economic Value Creation—or simply, EVC for short can be applied. The notion of EVC imparts summing together each of fundamental areas in which a technology, or group of technologies, adds value to the efficiency equation. Technology, by design, should make business operations more efficient when it displaces or augments a process that enhances productivity or constrains cost. When talking about efficiency, it is important to recognize that the concept implies three different approaches: *technical*, *operational* and *economic*. *Technical* efficiency—in the context of firewalls, information asset protection and general network security provisions—relates to the change at which technology alters the risk equation as a direct consequence of the technology additive. Firewalls enhance technical efficiency by reducing the negative by-products of attack and breach with respect to ensuring the continuation of normal business operations. If the technology was not in place, and an attack or breach was to occur, then business production would be disrupted either directly or indirectly. In any case, the ability of your organization to produce its goods or services at the same rate would be lessened—if not ceased momentarily. Complementary to technical efficiency advantages, the approach of *operational* efficiency concerns itself with the configuration of capital, infrastructure and the resources necessary to maintain

business operations. When support staff burdens themselves with the added labor and resources required in correcting a negative security outcome, this takes away valuable productivity that would otherwise be applied to normal business operations.

Technology that aids or preserves resources within the business configuration is said to improve operational efficiency—following the old adage of 'doing more with less'. Operational efficiency is vital when contemplating the labor input necessary to maintain a network environment, especially from the aspect of supporting end-users and strategic projects that come before recovery operations. When most technology vendors discuss efficiency, what their message often conveys is that the solution will save money—or more appropriately, minimize costs. But saving money is only a small part of *economic* efficiency when assessing the incremental capacity to minimize capital expenditures or maximize revenue. At face value, technology should conserve at least some resources when selected to replace inefficiency or enhance revenue opportunity. Network security not only protects companies from the costly expenditures associated with cleanup and recovery from attacks, but it can also drive productivity above and beyond normal levels by enabling network assets to perform more effectively. And effective networks translate to bottom line improvement on a real cash basis. Taking each of these efficiency approaches separately and together, EVC creates a different picture of the value proposition by addressing the investment from a contemporary angle. Technical efficiency drives companies to mitigate risk by lowering their probability for network violation and allocating their productive resources more diligently. Operational efficiency ensures that the configuration of capital and infrastructure continues to perform as scheduled and that labor resources are best applied to their respective tasks. Economic efficiency drives performance in the financial quadrant and helps companies realize revenue opportunities through reliable networks with predictable Quality of Service (QoS). And measured jointly, the view toward making a business case for network security becomes sharpened across each context.

Descriptive Statistics and the Economics of Network Violations

True costs of network disruptions—from multiple sources—has been historically difficult to measure and quantify since many of the repair costs are buried within the accounting systems of the victim organizations. And without an aggregated source of data relevant to such attacks, or statistical estimators that probe the ranges of actuarial cases, the design of macroeconomic interpretation was made on a lower confidence interval scale. Data is quite abundant and prominent code-level destruction spans the globe almost weekly. Anti-virus and pattern recognition companies such as Entercept and Symantec have carved a historian's position in recording the deluge of passive code-level attacks that flourish daily. But in an economic sense, the real damage of attacks and malicious behaviour takes shape as an *externality* of network-based computing. With open access to the Internet and information assets at risk, these attacks will continue to propagate and spread themselves in new hybrid platforms that will challenge the best firmware

appliances and software developers alike. Some of the empirically relevant figures and statistics that define this externality include:

Historical Lessons of Failure and Conclusion

Dating back to the early 1980s when hacker popularity began to rise, the commonality of PC security gave attention to the explosion of viruses that sprung up overnight in the midst of a booming personal technology revolution. Historical economists that look at past trends and determine their causal patterns have noted that malicious behaviour coincides with peak economic periods during which significant advances in technology accompany surges in personal wealth. And next to these upturns in economic activity, vulnerability is at its highest level when organizations stay focused on wealth building activities and develop complacency for lax security procedures. Today's technology has crossed over into new landscapes with network connectivity becoming central to emerging technologies in both enterprise and personal markets. This leads us to conclude that the network will be the most likely conduit for dispersal of passive code-level attacks and the Internet its global theatre for terrorism in higher order. To protect against forthcoming intrusion and misappropriation of digital assets, organizations need to make a clear resolve in their expenditures toward security concentration within the network domain. Security is a rational element of business operations, but until recently, many had forgotten just how important this application could be in preserving the modern day enterprise.

Self Assessment Exercise

a. What do you understand by dominant risk outcomes?
b. How can they be categorized?

4.0 Conclusion

Risk is always present at the epicentre of network computing and how a company faces risk can drastically alter their future. Begin by defining risk in terms that encompass your IT constituency. Then, use some of the parameters presented herein this appraisal to

guide your measurement of the risk horizon. And once you determine the focus of risk mitigation, seek technologies that will serve an economic value in reducing that risk quotient.

5.0 Summary

As an economic appraisal of network security attacks and vulnerability to digital intrusion—this unit sets forth to define components of risk mitigation through the investment in firewall appliances and server-side preservation technologies. Aside from descriptive statistics that illuminate real-world occurrences, the numerical values contained herein can be applied to nearly every organization seeking to lower their economic risk associated with information technology compromise and justify nominal expenditures for securing their assets. Security can no longer be regarded as an auxiliary technology investment, but rather as a core investment in the capitalization of the enterprise business model— alongside the host of other inputs that ensure business output and productivity.

6.0 Tutor Marked Assignment

Define the term risk , its *measurement* and *mitigation?*.

7.0 References/ Further Reading

Bishop, M (2002). " Computer Security Art and Science", Pearson/PHI, USA

CERT, (1999). Results of the Distributed-Systems Intruder Tools Workshop, Software Engineering Institute, Carnegie Mellon University, http://www.cert.org/reports/dsit_ workshop-final.html, December 7.

Curtis, W; Krasner, H; Iscoe, N. A Field Study of the Software Design Process for Large Systems", in *Communications of the ACM* v 31 no 11 (Nov 88) pp 1268{1287.

Denning D. E (1999) Information Warfare and Security. ACM Press, USA.

Krause, M., and Harold, F. T, (2004). " Handbook of Information Security Management", Vol 1-3 CRC Press LLC.

McClure S, Scrambray, J., Kurtz, G. (2003). "Hacking Exposed", Tata McGraw-Hill.USA

Varian, H. (2000). Managing Online Security Risks. Economic Science Column, The New York Times, June 1, 2000, http: //www.nytimes.com/library/financial/ columns/060100econ scene.html.

Module 4

Unit 1. Information Age Militaries
Unit 2. Information Technology Impacts on War fighters
Unit 3. Information Technology and Nature of Future War
Unit 4. Difficulties in Information Security
Unit 5. The Economics of Information Security Investment

Unit 1
Information Age Militaries

Contents

1.0 Introduction

Military operations in the future will be conducted by Information Age organizations. Unlike today's military organizations that would be reasonably familiar and comfortable to 19th-century warriors, Information Age militaries will be more of a reflection of contemporary private sector organizations. Information Age militaries will differ from 20th-century militaries with respect to their (1) strategy, (2) degree of integration, and (3) approach to command and control.

2.0 Objectives

Students are expected to understand how the information age will impact on the military, its strategies and operations. Similarly students are expected to highlight the importance of information system age on military Integrated Operations.

3.0 Main body

Military Strategy

Military strategy has, until recently, been basically symmetric with the aim of degrading and/or defeating an adversary's military forces. To some extent, military operations have been a separate phase in a conflict that begins when the political leadership turns to a military organization and expects it to undertake and accomplish a given military mission. Upon the conclusion of this mission (e.g., surrender of the enemy), the military retires and the political leadership takes over. This is not to say that civilian leadership is not engaged during the entire military phase, but that the role of civilian leadership during the conduct of military operations is more of an oversight role, not an operational one. Conflicts in the Information Age will not have distinct military phases to the same extent as before. Military objectives will need, more than ever before, to be dynamically balanced with a set of nonmilitary objectives and subject to a complex set of constraints. Hence, military strategy will need to adjust to being a part of a larger operation and

switch to an effects based strategy (as opposed to an attrition-based strategy). The term *effects-based operations* (EBO) is relatively recent, although one would hope that warfare has always been about creating effects. However, in the Industrial Age, attrition effects became an automatic substitute for the ultimate objectives of military operations. As nontraditional military missions became more commonplace, it became obvious that new measures of effectiveness for military operations needed to be developed. Enemy attrition and loss exchange ratios were no longer useful. EBO is simply a recognition of this. Its proponents are arguing for an explicit enunciation of the objectives of a military operation, how these military objectives relate to overall U.S. or coalition objectives, and the cause effect relationships that link military actions to effects to military objectives to mission objectives. Normalcy indicators, for example, may be used to ascertain when a peacekeeping mission achieves the desired effects. In these cases, military actions (e.g., patrols, weapons confiscation) need to be related to normalcy. Killing people and breaking things may, in fact, be part and parcel of an effects-based strategy, but this connection should not be casually assumed. Much has been written on this change in the relationship of the military to conflict.

Command and Control: Integrated Operations

While the Information Age will complicate military strategy, it will revolutionize military organizations and the approach to command and control. Command and control is a military term for leadership and management. Improvements in Information Age technologies have changed the economics of information and hence, have altered its practical richness, reach, and the quality of the interactions among individuals and groups. As a result, the nature of the fog and friction of war are being radically altered. This will enable us to move beyond the pursuit of blunder avoidance and deconfliction to achieving synergy on a routine basis in military operations. Curiously, the term *integration* is not part of the dictionary definition of management, although it seems to me that a key component of management lies in its ability to integrate the actions of an organization. Information Age militaries will be able to generate synergy because they will be better integrated in a number of dimensions. These dimensions include echelon, coalition/joint, function, time, and geography. The infinitive *to integrate* is commonly defined as “to make a whole by bringing all parts together.” Military operations traditionally break each of the dimensions mentioned above into parts that have for the most part not been brought together very well. This approach creates seams on the battlefield that an adversary can exploit. Military tactics recognize that the seam between units (particularly if the seam separates troops from different countries as they often did in World War II) is a good place to attack. Information and opportunity find the cracks in the seams irresistible.

The real challenge in command and control is integration. It is about getting a number of things to work toward a common purpose in a way that maximizes the totality of the resources available. This raises an interesting point about integration. Is integration about the means employed, or is it only about the effects produced? Can an organization be

integrated without achieving integrated effects? If an organization achieves integrated effects, is it integrated? Take the idea that is central to Information Age command and control, self-synchronization. Are self-synchronizing forces integrated? These questions are important because they help us focus attention in the right places. The argument therefore that is that self synchronizing forces (e.g., those that achieve synchronized results by emergent behavior), are indeed integrated because, in the final analysis, they achieve integrated effects by enabling individuals to develop synergistic behaviors. Synchronized behavior can also be a product of centralized planning and execution, or of centralized planning and decentralized execution.

The way command and control should be exercised in the Information Age depends upon what actually works best in the set of circumstances and challenges we associate with today's and tomorrow's military missions. Information Age missions will be characterized by a large degree of unfamiliarity and complexity, and by exacting time pressures and constraints. They will require rapid, decisive, and precise responses. The ability to rapidly respond is limited by physics unless one shifts to an approach involving the massing of the desired effects rather than the massing of forces. This, in turn, means that forces can be geographically dispersed. Dispersion of forces may result from either the inability to mass physically in time or a desire to maintain separation to avoid being an attractive target. Being decisive involves, among other things, being able to select the right effects and develop a feasible approach for achieving them. This requires a high level of understanding of the situation. *Precise* means that each element or part of the force knows if, when, and how to act and has the capability to achieve the desired effects. Rapid, decisive, and precise responses can only be accomplished if we are able to bring all of the available information we have to bear and all available assets to bear in a timely manner.

Self Assessment Exercise
Explain the relevance of the information age to military strategies.

4.0 Conclusion
The conditions necessary for success in the Information Age revolve around an organization characterized by information flows that are not unduly constrained, where the key parts of the organization share awareness, and where acts of individual parts can be self-synchronized. These are characteristics that are associated with integrated processes. This can only be achieved by adopting a network-centric approach and command philosophy.

5.0 Summary
This unit highlights information age militaries, military operations and projects into the future organizations of military. It emphasizes the fact that in time to come military operations will be conducted using more of tactics and strategies based on information system technologies, which will require rapid, decisive, precise and accurate responses.

6.0 Tutor Marked Assignment

Explain why integration is commonly referred to as the real challenge in command and control.

7.0 References/ Further Reading

Alberts, D. S. and Papp, D.S. (2001), *Information Age Anthology*. Washington, DC: National Defense University and CCRP. June 1997-March 2001. Vols 1-3.

Alberts, David S. and Hayes. R.E. (1995) *Command Arrangements for Peace Operations*. Washington, DC: National Defence University. May 1995. pp. 5-13.

Alberts, D.S., Garstka, J.J., Hayes, R.E. and Stein. F.P. (1999). *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington, DC: CCRP. August 1999.

Alberts, D.S., Garstka, J.J., Hayes, R.E. and Signori, D.A. (2001).*Understanding Information Age Warfare*. Washington, DC: CCRP. August

CNN: http://www.cnn.com/2002/US/01/31/rumsfeld.speech/index.html. January 31, 2002.

Fagin, Robert and Chris Kwak. *Internet Infrastructure and Services*. Bear Stearns, May 2001.

Garamone, J. (2002) "Flexibility, Adaptability at Heart of Military Transformation." *American Forces Press Service*. Jan 31, 2002.

Hayes, M. D and Gary F. (1996).Wheatley, eds. *Interagency and Political-Military Dimensions of Peace Operations: Haiti—A Case Study*. Washington, DC: National Defense University. February

Network Centric Warfare Department of Defense Report to Congress. July 2001. pp. 12-14.

Unit 2

Information Technology Impacts on War fighters

Contents

1.0 Introduction

Information technologies, for the purposes of this analysis, include collection, processing, display, and communications technologies. Processing technologies include data fusion and analysis, as well as support for decision-making and sense making, such as knowledge based expert systems and systems that support cognition. Display technologies include visualization tools and techniques.

2.0 Objectives

Students are expected to understand the impact of:

1. Information Technology on Warfare and
2. Networking and wireless technologies in war time scenario

3.0 Main body

Advances in these technologies have resulted in an enormous amount of near real-time information being potentially available to individuals anywhere at any time. The intelligence level of systems and our confidence in their ability has also increased dramatically to the point where life-and-death decisions are now routinely being made automatically by computers, albeit with varying degrees of human supervision. Even at this early point in the Information Age, the battlefield is awash with vastly improved quality and increased amounts of information. The dynamics of information dissemination have changed considerably in the latter half of the 20th century, from flowing primarily through organizational hierarchies or command structures to the point where significant amounts of information are obtained outside of these vertical flows and increasingly from non-security sources. Thus, what was once predominantly a highly constrained and vertical information flow has evolved into a mix of vertical and horizontal flows that extends beyond traditional security. And more, much more is still to come. Networking and wireless technologies have untethered us both organizationally and geographically. We are on the verge of “Internet 3.0,” which incorporates a set of

distributed capabilities (processing, storage, network services, and collaborative environments) that enable peer-to-peer (P2P) and dynamically reconfigurable small group interactions (collaborations). Solutions to dealing with today's information flows will not necessarily work with tomorrow's vastly increased flows. The amount, quality, and dynamics of information dissemination have already begun to impact the ways decisions are allocated (delegation) and the manner in which those decisions are made.

Network Centric Warfare (NCW) is all about changing decision-making processes and topologies. It involves moving from an Industrial Age model, where information is collected at the edges and moved to the center for decision-making, to an Information Age model, where the edge is empowered to make decisions based upon command intent and high quality situation awareness. The effectiveness of an Industrial Age organization depends upon the decision-making ability of one person (or a small number of persons) at the center and the ability to parse and communicate decisions, in the form of guidance, to subordinates such that their actions are synchronized. Thus, centralized deliberate planning has been the traditional focus of command and control systems. Early in the Information Age, information technologies were employed to incrementally improve this traditional command and control process. With NCW, there has been a focus on replacing the traditional command model with a new one—one based upon self synchronization enabled by shared awareness. Thus (as shown in Figure 1), advances in information technologies provide us with significant opportunities both to improve our ability to command and control our forces and to improve our force capabilities.

Information Age Transformation

Figure 1. The New Environment

Our information-related vulnerabilities have also increased. Increased reliance on high-tech systems for information collection, interpretation, processing, analysis, communication, and display has made failures in these systems more disruptive. The ubiquitous nature of these technologies provides our potential adversaries with capabilities that help them understand how to attack our information assets and give them the tools to do so.

Military command and control systems can no longer be evaluated using measures of merit (MOMs) related solely to the production of quality information in a timely manner. It is now important to consider such attributes as availability, integrity, and authenticity of the information, its ease of use, and its value-added for decision-making. Command and control has long been a recognized force multiplier, and improvements in information technologies offer tremendous opportunities to perfect existing approaches and explore new ones. Quicker, better decisions will allow us to operate more effectively within the enemy's decision cycle, providing us with an opportunity to control engagements. This is referred to as the speed of command. Improvements in information technologies also enhance the capabilities of human weapons, providing them with increased standoff capability and accuracy. Experiences in Afghanistan have shown that when forces can interoperate in new and innovative ways, good things happen. The key battle of Mazar-e-Sharif was, in the words of the Secretary of Defense, a combination "of the ingenuity of the U.S. Special Forces, the most advanced, precision-guided munitions in the U.S. arsenal delivered by U.S. Navy, Air Force, and Marine Corps crews, and the courage of valiant one-legged Afghan fighters on horseback."

But the opportunities that new, improved, and interoperable weapons and command and control systems offer cannot be successfully exploited unless we rethink our concepts of operations and our approach to command and control, change processes, doctrine, and organizational structures, and provide the required personnel the education, training, and experiences they need. This theme was stressed in a speech that Secretary Rumsfeld gave to students at the National Defense University in which he said, "A revolution in military affairs is about more than building new high-tech weapons, though that is certainly part of it. It's also about new ways of thinking, and new ways of fighting." Dealing with disruptive innovation is, to many, a daunting prospect. But, as the remainder of this book will show, we have no alternative but to treat the adoption of new information-related capabilities holistically, that is, to consider them in a mission capability package context.

A major issue is the pace of change expressed, for example, by Moore's Law (1962). With new capabilities being available so quickly, how can we possibly learn to effectively use these capabilities before they, in turn, become obsolete? The answer lies in a transformation strategy that anticipates technology, rather than trails technology. This approach is concept-driven rather than technology-driven. We do not have to wait for improvements in technology to actually occur before considering new approaches to command and control, concepts of operation, doctrine, or organizational arrangements.

Quite the contrary, if we wait, the inertia associated with developing and implementing these changes will keep us permanently behind the power curve. This does not imply that changes in command and control or force capabilities must necessarily precede alterations to concepts of operation or doctrine. In reality, these elements (e.g., concept of operations, doctrine, technology, etc.) constitute a package that, taken as a whole, provides real operational capability that can be applied in a specific mission.

Self Assessment Exercise

1. Discuss the term information vulnerabilities?
2. What are the issues in Information Age Transformation? Explain with the aid of a diagram.

4.0 Conclusion

A mission specific perspective is important because no organizational structure or approach to command and control is going to be well-suited for the range of likely missions; missions as diverse as traditional major theater wars (MTWs), small-scale contingencies, counter-terrorism, and peace operations. New measures of merit (MOMs) will be required that must be mission-related. For example, classic measures, such as attrition or taking and holding territory, are not relevant in many mission contexts. In addition to the need to employ metrics that reflect success in nontraditional missions (e.g., normalcy indicators for operations other than war (OOTW)), the very broad spectrum of missions that the military may be called upon to undertake and the uncertainties associated with them give rise to a need for metrics that reflect agility.

5.0 Summary

This unit examines advances in information technologies a departure from traditional focus of command and control systems in warfare. It highlights the relevance of Network Centric Warfare in decision-making processes as well as the topologies, and models in Information Age.

6.0 Tutor Marked Assignment

What do you understand by Network Centric Warfare (NCW)?

7.0 References/ Further Reading

Alberts, D.S. (1996). *The Unintended Consequences of Information Age Technologies: Avoiding the Pitfalls, Seizing the Initiative*. Washington, DC: National Defense University. April

Alberts, D.S., Garstka, J.J., and Stein F.P. (1999). *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington, DC: CCRP. August

CNN: http://www.cnn.com/2002/US/01/31/rumsfeld.speech/index.html. January 31, 2002.
Network Centric Warfare Department of Defence Report to Congress. July 2001. pp. 12-14.

Fagin, Robert and Chris Kwak. *Internet Infrastructure and Services*. Bear Stearns, May 2001.

Jim Garamone. “Flexibility, Adaptability at Heart of Military Transformation.” *American Forces Press Service*. Jan 31, 2002.

Unit 3

Information Technology and Nature of Future War

Contents

1.0 Introduction

Future war can be envisioned as consisting of three general classes of activities. First, there is the perfection of traditional combat. Second, there is the evolution of what has been called nontraditional missions, a very mixed bag of activities including humanitarian assistance, SOLIC (Special Operations and Low Intensity Conflict) operations, counter-drug operations, peace operations, and counter proliferation. Third, there is the birth of a form of war unique to the Information Age.

2.0 Objectives

Students are expected to know

1. the Future Traditional Combat as a means of security,
2. Evolution of Nontraditional Missions and its implication on Warfare..

3.0 Main body

Information technology will not only change the nature of what we know today as war and operations other than war (OOTW), but also will spawn a new set of activities that will become familiar to future generations as constituting warfare in the 21st century. Today we might have some difficulty in viewing this set of activities as war or as the concern or responsibility of militaries. Current planning and budgeting approaches, as well as research and development activities, find it difficult to address these aspects of the future since they are not extensions of existing military missions and responsibilities. However, in each of these three cases, information technologies and the adaptations to the capabilities they provide will shape the battlespace and redefine the possibilities.

Future Traditional Combat

The future conventional battlespace will be neither contiguous nor orderly. Tempo will be extraordinarily high by today's standards. Given expected improvements in weapons

and command and control, if a target can be seen, it can be destroyed. It should be noted that, more than ever, simply being able to destroy a target does not mean that one should do so. A variety of other considerations will determine the appropriate action to take. Some of these considerations will be the possibility of collateral damage, the link between the target and the effects desired, and the availability of non-lethal means. Survival of targets will depend upon organic defensive capabilities, suppression, and stealth. Concepts of operation will center around massing effects1 rather than forces. Command and control involves dynamic tradeoffs between ensuring that Rules of Engagement (ROE) are followed, prioritizing targets, and minimizing the time required for shooters to pull the information they need. While commanders will have the ability to exert more direct influence on shaping the battlespace, they may wish to not exercise this option. Network Centric Warfare (NCW) theory argues that, in certain kinds of situations, it is more effective to opt for a network-centric or self-synchronizing approach with the commander focused on influencing the initial conditions of the engagement rather than micromanaging it. If the experience of other organizations holds, staffs (as we now know them) will be significantly reduced (and decentralized) as organizational structures flatten. Many commands will be automatically disseminated and incorporated in decision aids. Many decisions will be fully automated. Virtually all information will be distributed horizontally. In short, many significant changes will need to be made in the way we think about command and control to respond to the challenges of the Information Age. With this much change foreseen down the road, care must be exercised to ensure success, even for the set of missions that we know best.

Evolution of Nontraditional Missions

Since the end of the Cold War, America has looked inward not only to reduce overall spending, but also to undertake a more diverse set of roles, both at home and around the globe. The unique capabilities developed by the U.S. military to meet the global challenge posed by the Soviet Union and maintained to protect their. interests around the world are seen as national assets that can be employed beyond their traditional combat and combat service support roles. Global air- and sea-lift are important for disaster relief, crisis intervention, humanitarian assistance, and support to peace operations. Similarly, the secure global communications capacity of the U.S. military is a crucial asset in a wide range of situations. The capability of the military to surge from its training bases and to react rapidly when dangerous situations arise far exceeds the capacities of most civilian agencies for whom surge capacity is a slow and cumbersome process and crisis response is an alien practice. These unique capabilities, combined with the absence of an urgent, traditional military threat have, until September 11, 2001, caused the nation to expect greater involvement in nontraditional missions such as humanitarian assistance, maintaining law and order when local and state authorities cannot, disaster relief, as well as countering drug smuggling and the proliferation of weapons of mass destruction.

The events of September 11, 2001, have shifted the priority from traditional combat to terrorism and dealing with nations that host and support terrorists. As its first priority,

must focus on the nexus of terror and Weapon of Mass Destruction. Clearly, this is very different from a focus on traditional combat and will require changes that go well beyond those that are involved in any adaptations to Information Age technologies. The international environment has also changed in ways that make nontraditional missions more likely and more diverse. Coalition operations are now the accepted norm rather than the exception. International organizations, particularly the United Nations, have become increasingly assertive and have pressed a vision of global interests in peace and cooperation. As the only remaining global superpower, the United States is expected to respond whenever international peace and harmony are threatened and the nations of the world feel action is needed. This has been interpreted to mean that the U.S. must lead when the peace is threatened, international crimes are committed, or human tragedy looms. Parochial clashes and conflicts undercut this growing internationalism. Freed from the smothering constraints of communist governments, national movements in Eastern Europe and the former U.S.S.R. have proven willing to challenge the peace to seek independence. Nations in Africa have reasserted their interests, sometimes violently. Asia is the site of arms races and uncertain relations between nations. Domestic and international struggles for the long-term control of the Middle East oil wealth and the worldwide resurgence of fundamentalist Islam add to the dangerous international situation. Drug traffickers present a frustrating cross-border challenge. Recent attention has also focused on conflicts arising from environmental issues, particularly disputes over water rights, ocean areas, and transnational air pollution. Irrespective of these minimizing casualties, among both combat forces and civilians, is widely perceived as an important and achievable goal. At the same time, the military is expected to be effective by accomplishing missions precisely and quickly.

Warfare in the Information Domain

As the global society enters the Information Age, military operations are inevitably impacted and transformed. Satellite communications, video teleconferencing, battlefield facsimile machines, digital communications systems, personal computers, the Global Positioning System, and dozens of other transforming tools are already commonplace. At the same time nations military base have infused technological advances into operations at an ever-increasing rate, they have gone from being the driving force in information technology to being specialty users. By policy and by necessity, they have found themself in a new situation, relying on commercial-off-the-shelf (COTS) technology in order to acquire and field cost-effective systems. The widespread proliferation of Information Age technology, has contributed to a significant increase in vulnerability. The implications of warfare in the information arena (cyberspace) are enormous. First, national homelands are no longer sanctuaries by virtue of convention, distance, geography, or terrain. Physical borders are meaningless in cyberspace. Homelands and citizens can be attacked directly and even anonymously by foreign powers, criminal organizations, or non-national actors such as ethnic groups, renegade corporations, or zealots.

Traditional military weapons cannot be interposed between the information warfare threat and society. Even where traditional combat conditions exist (hostile military forces face one another in a terrain defined battle space), kinetic weapons are now only one part of the arsenal available to the adversaries. Indeed, electronic espionage and sabotage, psychological warfare attacks delivered via mass media, digital deception, and hacker attacks on the adversaries' command and control systems have been used and will increasingly be used to neutralize traditional forces and contribute in their own right to a concentration of effects at the crucial time and place in the battle space. Warfare in the Information Age will require enormously complex planning and coordination, very near real-time, vastly improved situation awareness, and the ability to share this awareness. Decision support systems will be required to filter and fuse information very rapidly to provide common operational pictures (COPs) and perform simple plan extensions and revisions almost automatically.

Self Assessment Exercise
What do you understand by traditional and nontraditional missions in global information age security?

4.0 Conclusion

Massive database and information exchange capabilities will be needed to track both friendly and enemy situations as well as rehearse and forecast battlespace dynamics. Accordingly, our dependence on information and the systems that produce it, carry it, and provide access to it will continue to grow. This reality of an ever-increasing dependence on information means that the military must be able to: 1. Protect its own information systems; 2. Attack and influence the information systems of its adversaries; and 3. Leverage information advantages to gain a competitive advantage in the domain of national security.

5.0 Summary

This units introduces students to the Future Traditional Combat as a means of security, it examines the Evolution of Non-traditional Missions and its implication on Warfare in an ever-increasing information age and Domain.

6.0 Tutor Marked Assignment
Explain the reasons why countries are shifting from traditional forms of security.

7.0 References/ Further Reading
Alberts, David S., John J. Garstka, and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington, DC: CCRP. August 1999. pp. 6, 36,
66.

Alberts, D.S. *The Unintended Consequences of Information Age Technologies: Avoiding the Pitfalls, Seizing the Initiative*. Washington, DC: National Defense University. April 1996. Pp. 63-4.

Alberts, D.S. *The Unintended Consequences of Information Age Technologies: Avoiding the Pitfalls, Seizing the Initiative*. Washington, DC: National Defense University. April 1996. p. 40.

Alberts, D.S. (1996). *Defensive Information Warfare*. Washington, DC: National Defense University. August.

CNN: http://www.cnn.com/2002/US/01/31/rumsfeld.speech/index.html. January 31, 2002.
Network Centric Warfare Department of Defense Report to Congress. July 2001. pp. 12-14.

Combelles S.P. *Target Bosnia: Integrating Information Activities in Peace Operations*. Washington, DC: CCRP and National Defense University. January 1998.

Fagin, R. and Kwak, C.(2001). *Internet Infrastructure and Services*. Bear Stearns, May.

Hayes, M. D and G. F. Wheatley, eds. *Interagency and Political-Military Dimensions of Peace Operations: Haiti—A Case Study*. Washington, DC: National Defense University. February 1996.

Jim Garamone. "Flexibility, Adaptability at Heart of Military Transformation." *American Forces Press Service*. Jan 31, 2002.

Wentz, Larry, ed. *Lessons from Bosnia: The IFOR Experience*. Washington, DC: CCRP and National Defense University. April 1998. pp. 167-187

UNIT 4
Difficulties in Information Security

Contents

1.0 Introduction

In a survey of fraud against autoteller machines, it was found that patterns of fraud depended on who was liable for them. In the USA, if a customer disputed a transaction, the onus was on the bank to prove that the customer was mistaken or lying; this gave US banks a motive to protect their systems properly. But in Britain, Norway and the Netherlands, the burden of proof lay on the customer: the bank was right unless the customer could prove it wrong. Since this was almost impossible, the banks in these countries became careless. Eventually, epidemics of fraud demolished their complacency. US banks, meanwhile, suffered much less fraud; although they actually spent less money on security than their European counterparts, they spent it more effectively. There are many other examples. Medical payment systems that are paid for by insurers rather than by hospitals failure to protect patient privacy whenever this conflicts with the insurer's wish to collect information about its clients. Digital signature laws transfer the risk of forged signatures from the bank that relies on the signature (and that built the system) to the person alleged to have made the signature. Common Criteria evaluations are not made by the relying party, as Orange Book evaluations were, but by a commercial facility paid by the vendor. In general, where the party who is in a position to protect a system is not the party who would suffer the results of security failure, then problems may be expected. A different kind of incentive failure surfaced in early 2000, with distributed denial of service attacks against a number of high-profile web sites.

These exploit a number of subverted machines to launch a large coordinated packet flood at a target. Since many of them flood the victim at the same time, the traffic is more than the target can cope with, and because it comes from many different sources, it can be very difficult to stop. Varian (1999), pointed out that this was also a case of incentive failure. While individual computer users might be happy to spend $100 on anti-virus software to protect themselves against attack, they are unlikely to spend even $1 on software to prevent their machines being used to attack Amazon or Microsoft. This is an example of what economists refer to as the `Tragedy of the Commons'. If a hundred peasants graze their sheep on the village common, then whenever another sheep is added

its owner gets almost the full benefit-while the other ninety-nine suffer only a small decline in the quality of the grazing. So they aren't motivated to object, but rather to add another sheep of their own and get as much of the grazing as they can. The result is a dustbowl; and the solution is regulatory rather than technical. A typical tenth- century Saxon village had community mechanisms to deal with this problem; the world of computer security still doesn't. Varian's proposal is that the costs of distributed denial-of-service attacks should fall on the operators of the networks from which the flooding traffic originates; they can then exert pressure on their users to install suitable defensive software, or, for that matter, supply it themselves as part of the subscription package. These observations prompted us to look for other ways in which economics and computer security interact.

2.0 Objectives

Students are expected to understand the difficulties therein information security from the perspectives of microeconomics: network externalities, asymmetric information, moral hazard, adverse selection, liability dumping and the tragedy of the commons.

3.0 Main body

Network Externalities

Economists have devoted much effort to the study of networks such as those operated by phone companies, airlines and credit card companies. The more people use a typical network, the more valuable it becomes. The more people use the phone system - or the Internet – the more people there are to talk to and so the more useful it is to each user. This is sometimes referred to as *Metcalfe's law*, and is not limited to communication systems. The more merchants take credit cards, the more useful they are to customers, and so the more customers will buy them; and the more customers have them, the more merchants will want to accept them. So while that networks can grow very slowly at first - credit cards took almost two decades to take off - once positive feed- back gets established, they can grow very rapidly. The telegraph, the telephone, the fax machine and most recently the Internet have all followed this model. As well as these physical networks, the same principles apply to virtual networks, such as the community of users of a mass-market software architecture. When software developers started to believe that the PC would outsell the Mac, they started developing their products for the PC first, and for the Mac only later (if at all). This effect was reinforced by the fact that the PC was easier for developers to work with. The growing volume of software available for the PC but not the Mac made customers more likely to buy a PC than a Mac, and the resulting positive feedback squeezed the Mac out of most markets. A similar effect made Microsoft Word the dominant word processor. A good introduction to network economics is by Shapiro and Varian (1998). For our present purposes, there are three particularly important features of information technology markets.

- First, the value of a product to a user depends on how many other users adopt it.

- Second, technology often has high fixed costs and low marginal costs. The first copy of a chip or a software package may cost millions, but subsequent copies may cost very little to manufacture. This isn't unique to information markets; it's also seen in business sectors such as airlines and hotels. In all such sectors, pure price competition will tend to drive revenues steadily down towards the marginal cost of production (which in the case of information is zero). So businesses need ways of selling on value rather than on cost.

- Third, there are often large costs to users from switching technologies, which leads to lock-in. Such markets may remain very profitable, even where (incompatible) competitors are very cheap to produce. In fact, one of the main results of network economic theory is that the net present value of the customer base should equal the total costs of their switching their business to a competitor.

All three of these effects tend to lead to "winner takes all" market structures with dominant firms. So it is extremely important to get into markets quickly. Once in, a vendor will try to appeal to complementary suppliers, as with the software vendors whose bandwagon effect carried Microsoft to victory over Apple. In fact, successful networks tend to appeal to complementary suppliers even more than to users: the potential creators of ‘killer apps’ need to be courted. Once the customers have a substantial investment in complementary assets, they will be locked in. (There are a number of complexities and controversies; see for example. But the above simplified discussion will take us far enough for now) These network effects have significant consequences for the security engineer, and consequences that are often misunderstood or misattributed. Consultants often explain that the reason a design broke for which they were responsible was that the circumstances were impossible: `the client didn't want a secure system, but just the most security I could fit on his product in one week on a budget of $10,000'. It is important to realize that this is not just management stupidity. The huge first-mover advantages that can arise in economic systems with strong positive feedback are the origin of the so-called ‘Microsoft philosophy’ of `we'll ship it on Tuesday and get it right by version 3'. Although sometimes attributed by cynics to a personal moral failing on the part of Bill Gates, this is a perfectly rational behaviour in many markets where network economics apply. Another common complaint is that software plat- forms are shipped with little or no security support, as with Windows 95/98; and even where access control mechanisms are supplied, as with Windows NT, they are easy for application developers to bypass.

In fact, the access controls in Windows NT are often irrelevant, as most applications either run with administrator privilege (or, equivalently, require dangerously powerful operating system services to be enabled). This is also explained simply from the viewpoint of network economics: mandatory security would subtract value, as it would make life more difficult for the application developers. Indeed, Anderson (2001), observes that much of the lack of user-friendliness of both Microsoft software and the Internet is due to the fact that both Microsoft and the Internet achieved success by

appealing to developers. The support costs that Microsoft dumps on users - and in fact even the cost of the time wasted waiting for PCs to boot up and shut down - greatly exceed its turnover. Network owners and builders will also appeal to the developers of the next generation of applications by arranging for the bulk of the support costs to fall on users rather than developers, even if this makes effective security administration impractical. One reason for the current appeal of public key cryptography may be that it can simplify development - even at the cost of placing an unreasonable administrative burden on users who are neither able nor willing to undertake it. The technical way to try to fix this problem is to make security administration more `user-friendly' or `plug-and-play'; many attempts in this direction have met with mixed success. The more subtle approach is to try to construct an authentication system whose operators benefit from network effects; this is what Microsoft Passport does. In passing, it is worth mentioning that (thanks to distributed denial of service attacks) the economic aspects of security failure are starting to get noticed by government. A recent EU proposal recommends action by governments in response to market imperfections, where market prices do not accurately reflect the costs and benefits of improving network security. However, this is only the beginning of the story.

Competitive applications and corporate warfare

Network economics has many other effects on security engineering. Rather than using a standard, well analyzed and tested architecture, companies often go for a proprietary obscure one - to increase customer lock-in and increase the investment that competitors have to make to create compatible products. Where possible, they will use patented algorithms (even if these are not much good) as a means of imposing licensing conditions on manufacturers. For example, the DVD Content Scrambling System was used as a means of insisting that manufacturers of compatible equipment signed up to a whole list of copyright protection measures. This may have come under severe pressure, as it could prevent the Linux operating system from running on next-generation PCs; but efforts to foist non-open standards continue in many applications from SDMI and CPRM to completely proprietary systems such as games consoles. A very common objective is differentiated pricing. This is usually critical to firms that price a product or service not to its cost but to its value to the customer. This is familiar from the world of air travel: you can spend $200 to fly the Atlantic in coach class, $2000 in business class or $5000 in ’first class. Some commentators are surprised by the size of this gap; yet a French economist, Jules Dupuit, had already written in 1849:

> *It is not because of the few thousand francs which would have to be spent to put a roof over the third-class carriage or to upholster the third-class seats that some company or other has open carriages with wooden benches . . . What the company is trying to do is prevent the passengers who can pay the second-class fare from travelling third class; it hits the poor, not because it wants to hurt them, but to frighten the rich . . . And it is again for the same reason that the companies, having proved almost cruel to the third-class passengers and mean to the second-class ones, become lavish in dealing with first-class*

customers. Having refused the poor what is necessary, they give the rich what is superfluous.

This is also a common business model in the software and online services sectors. A basic program or service may be available free; a much better one for a subscription; and a `Gold' service at a ridiculous price. In many cases, the program is the same except that some features are disabled for the budget user. Many cryptographic and other technical protection mechanisms have as their real function the maintenance of this differential. Another business strategy is to manipulate switching costs. Incumbents try to increase the cost of switching, whether by indirect methods such as controlling marketing channels and building industries of complementary suppliers, or increasingly, by direct methods such as making systems incompatible and hard to reverse engineer. Meanwhile competitors try to do the reverse: they look for ways to reuse the base of complementary products and services, and to reverse engineer whatever protection the incumbent builds in. This extends to the control of complementary vendors, sometimes using technical mechanisms. Sometime, security mechanisms have both product differentiation and higher switching costs as goals. An example which may become politicized is `accessory control'. According to one company that sells authentication chips into the automative market, some printer companies have begun to embed cryptographic authentication protocols in laser printers to ensure that genuine toner cartridges are used. If a competitor's cartridge is loaded instead, the printer will quietly downgrade from 1200 dpi to 300 dpi. In mobile phones, much of the profit is made on batteries, and authentication can be used to spot competitors' products so they can be drained more quickly.
Another example comes from Microsoft Passport. This is a system whose ostensible purpose is single sign on: a Passport user doesn't have to think up separate passwords for each participating web site, with all the attendant hassle and risk. Instead, sites that use Passport share a central authentication server run by Microsoft to which users log on. They use web redirection to connect their Passport-carrying visitors to this server; authentication requests and responses are passed back and forth by the user's browser in encrypted cookies. So far, so good. But the real functions of Passport are somewhat more subtle. First, by patching itself into all the web transactions of participating sites, Microsoft can collect a huge amount of data about online shopping habits and enable participants to swap it. If every site can exchange data with every other site, then the value of the network to each participating web site grows with the number of sites, and there is a strong network externality. So one such network may come to dominate, and Microsoft hopes to own it.

Second, the authentication protocols used between the merchant servers and the Passport server are proprietary variants of Kerberos, so the web server must use Microsoft software rather than Apache or Netscape (this has supposedly been `mixed' with the latest release, but participating sites still cannot use their own authentication server, and so remain in various ways at Microsoft's mercy). So Passport isn't so much a security product, as a ploy for control of both the web server and purchasing information markets.

It comes bundled with services such as Hotmail, is already used by 40 million people, and does 400 authentications per second on average. Its known flaws include that Microsoft keeps all the users' credit card details, creating a huge target; various possible middleperson attacks; and that you can be impersonated by someone who steals your cookie file. (Passport has a `logout' facility that's supposed to delete the cookies for a particular merchant, so you can use a shared PC with less risk, but this feature didn't work properly for Netscape users when it was first deployed.) The constant struggles to entrench or undermine monopolies and to segment and control markets determine many of the environmental conditions that make the security engineer's work harder. They make it likely that, over time, government interference in information security standards will be motivated by broader competition issues, as well as by narrow issues of the effectiveness of infosec product markets (and law enforcement access to data). So much for commercial information security. But what about the government sector? As information attack and defence become ever more important tools of national policy, what broader effects might they have?

Information Warfare - Offense and Defence

One of the most important aspects of a new technology package is whether it favours offence or defence in warfare. The balance has repeatedly swung back and forth, with the machine gun giving an advantage to the defence in World War 1, and the tank handing it back to the offense by World War 2. The difficulties of developing secure systems using a penetrate-and-patch methodology have been known to the security community since at least the Anderson report in the early 1970s; however, a new insight on this can be gained by using an essentially economic argument that enables us to deal with vulnerabilities in a quantitative way. So information warfare looks rather like air warfare looked in the 1920s and 1930s. Attack is simply easier than defence. Defending a modern information system could also be likened to defending a large, thinly-populated territory like the nineteenth century Wild West: the men in black hats can strike anywhere, while the men in white hats have to defend everywhere. Another possible relevant analogy is the use of piracy on the high seas as an instrument of state policy by many European powers in the sixteenth and seventeenth centuries. Until the great powers agreed to deny pirates safe haven, piracy was just too easy. Finally - and this appears to be less widely realized - the balance in favour of attack rather than defence is still more pronounced in smaller countries. They have proportionally fewer citizens to defend, and more foreigners to attack. In other words, the increasing politicization of information attack and defence may even be a destabilizing factor in international affairs.

Self Assessment Exercise

What do you understand by the concept Network Externalities?

4.0 Conclusion

Much has been written on the failure of information security mechanisms to protect end users from privacy violations and fraud. This misses the point. The real driving forces behind security system design usually have nothing to do with such altruistic goals. They are much more likely to be the desire to grab a monopoly, to charge different prices to different users for essentially the same service, and to dump risk. Often this is perfectly rational. In an ideal world, the removal of perverse economic incentives to create insecure systems would de- politicize most issues. Security engineering would then be a matter of rational risk management rather than risk dumping. But as information security is about power and money -about raising barriers to trade, segmenting markets and differentiating products - the evaluator should not restrict herself to technical tools like cryptanalysis and information flow, but also apply economic tools such as the analysis of asymmetric information and moral hazard. As fast as one perverse incentive can be removed by regulators, businesses (and governments) are likely to create two more. In other words, the management of information security is a much deeper and more political problem than is usually realized; solutions are likely to be subtle and partial, while many simplistic technical approaches are bound to fail. The time has come for engineers, economists, lawyers and policymakers to try to forge common approaches.

5.0 Summary

This unit highlights as well as discusses some of the major difficulties in information security, such as Network Externalities, Competitive applications and corporate warfare, and Information Warfare. Emphasis was placed on Network economics and its effects on information security usage and cost.

6.0 Tutor Marked Assignment

Succinctly discuss some of the difficulties in Information Security

7.0 References/ Further Reading

Akerlof, G. A (1970). The Market for 'Lemons': Quality Uncertainty and Market Mechanism," Quarterly Journal of Economics Vol. 84 pp 488-500

Anderson, J. (1973) *`Computer Security Technology Planning Study'*, ESD-TR-73-51, US Air Force Electronic Systems Division
http://csrc.nist.gov/publications/history/index.html

Anderson, R.J (2001) *`Security Engineering - A Guide to Building Dependable Distributed Systems'*, Wiley ISBN 0-471-38922-6.

Bloom, J.A., Cox, I.J., Kalker, T., Linnartz, J., Miller, M.L., Traw, CBS (1999). Copy Protection for DVD Vide, in *Proceedings of the IEEE* Vol. 87 No. 7 Pp 1267-1276.

Brady, R.M., Anderson, R.J., Ball, R.C. (1999). *`Murphy's law of evolving species, and the lim- its of software reliability'*, Cambridge Univer- sity Computer Laboratory Technical Report no. 476 at http;//www.cl.cam.ac. uk/~rja14.

Curtis, W., Krasner, H., Iscoe, N.A., (1988) Field Study of the Software Design Process for Large Systems, in *Communications of the ACM* . V 31no 11 pp 1268-1287

Kormann, D.P, and Rubin, A.D. (2000). Risks of the Passport Single Sign-on Protocol", in *Computer Networks* (July 2000); at http://avirubin. com/vita.html

Liebowitz, S.J., Margolis, S.E \Network Externalities (Effects)", in *The New Palgrave's Dic-*
tionary of Economics and the Law, MacMillan, 1998; see
http://wwwpub.utdallas.edu/liebowit/netpage.html

Lloyd, W.F. (1833) *`Two Lectures on the Checks to Population'*, Oxford University Press 38-46, at http://www.acm.org/networker/issue/9805/ssnet.html

Shapiro, C. and Varian, H, (1998), *`Information Rules'*, Harvard Business School Press ISBN
0-87584-863-X

Varian, H. (1999). *Intermediate Microeconomics- A Modern Approach'*, Fifth edition, WW Norton and Company, New York,; ISBN 0-393- 97930-0

Varian, H. Managing Online Security Risks", Economic Science Column, The New York Times, June 1, 2000, http://www.nytimes.com/library/financial/ columns/060100econ-scene.html.

UNIT 5

The Economics of Information Security Investment

Content

1.0 Introduction

2.0 Objectives

The main aim of this unit is to provide students who will eventually be saddled with decision making responsibilities with a set of requirements to be considered when implementing a cost-effective and optimal information security budget; in a manner that preserve organisations' information security posture and compliance status.

3.0 Main body

Information security is a continuously changing discipline that requires continuous adaptation to new and ever-changing information security threats, countermeasures and the global business landscape. The global business landscape is on the verge of facing a recession following the ongoing global economic turmoil. This came as a result of the collapse of the United States of America's sub-prime mortgage market. Organisations must quickly adapt to the prevailing economic climate by becoming more vigilant in their spending in general and more so on overheads such as information security expenditure. Alas, despite the lingering global economic turmoil and encouraging developments in information security, a survey conducted by Symantec in 2008 revealed that the global underground economy is booming at millions of dollars in advertised goods and services. While the whole world is in the worst economic crisis, the underground economy continues to flourish. Despite all the years of hard work on information security technology improvements, harsh compliance regulatory penalties and more coordinated law enforcements, information security breaches are still ubiquitous and have seriously damaging consequences Clearly, something is not working effectively in the information security arena. Are the organisations putting in enough effort to protect their information assets or are they not taking any precautions? Is it too little or just enough or more? How much is really enough? The field of economics of information security has become an important field of study. For the past decade, researchers have identified several topics of interest but this unit focuses only on the economics of information security investment.

The Economics of Information Security Investment

This unit focuses on the topic 'information security investment' which is viewed from two opposing perspectives: either from the system defender's or the attacker's point of view. Investing in information security is a trade-off; organisations can either choose to invest in security or not to invest. There are both direct and indirect benefits and costs involved. Directly, investing in information security reduces the risk exposure – though at an opportunity cost of other profitable investment. Not investing in information security guarantees more money – but at an opportunity cost of not having secure information assets. Indirectly investing in information security can help those who have not invested to "a free ride". Those who do invest could easily become victims of threats that come from those who fail to invest (what economists call externality). Information security practitioners have to consider the trade-offs and related issues when they scrutinise and make information security investment decisions. Given the current threat landscape, the consequences of not investing in information security can prove to be more costly than the consequences of investing. Chapman (2009) highlight that organisations are losing billions of dollars because of information security breaches. The amount of time and effort that is involved in recovering from an information security breach, besides compliance fines and penalties to be paid is also a cause of concern. Over the years, organisations have therefore been left with no option but to invest in information security.

An Optimal Allocation of Funds to Information Security

Organisations need adequate information security at a reasonable cost. For information security to make business sense; organisations must strike the right balance between the likelihood of risk and the cost to reduce such risk (Su, 2006). This has proven not an easy task to do. Goetz and Johnson (2006) point out that a majority of executives view information security as a "bottomless pit that never gets full" and some see it as "necessary evil that hinders productivity" This is mainly due to the failure of information security managers to quantify their expenditure and the likelihood of the risk, faced by the information assets materialising. This failure has led executives to ask "how much is really enough for information security?" In answering the fore-going question and contrary to the views of "a bottomless information security pit that never gets full"; researchers argue that there is actually an optimal point for information security spending which several researchers have tried to determine. It is not advisable to invest below or beyond this point. Huang et al. (2006) use an economic model to determine optimal information security spending for organisations under multiple attacks. Modelling with variables such as system vulnerability, potential loss, budget and investment effectiveness, they demonstrate how to optimally allocate information security investments. Wang and Song (2008) propose modelling with information security requirements, opportunity costs of the risks and budget constraints. They use a multi-objective decision-making framework to determine the optimal information security investment. Unfortunately, the modelling approaches discussed in both Huang et al. (2006) and Wang and Song (2008) do not provide a definite figure or the exact point of

optimality for an information security investment. Srinidhi et al. (2008) also present a model to assist information security managers to optimally allocate financial resources to information security so as to guarantee productivity and the safety of information assets. In 2002, Gordon and Loeb proposed an economic model (G&L model hereafter) to determine the optimal allocation of funds among different assets with different vulnerabilities to information security. Unlike the work of Huang et al. (2006) and Wang and Song (2008), their findings show that the optimal investment for protecting an information asset must at least be less than or equal to 37% of the total loss expected of the information asset. Willemson (2006) reviewed and refuted the G&L model's claim. Relaxing this model's assumptions, Willemson provided a function that suggests an investment of up to 50% and even up to 100% of the expected loss of an information asset. Tanaka, Matsuura and Sudoh (2005) subsequently conducted an extensive empirical study using the G&L model. Their work investigates the relationship between information sharing and vulnerability levels and how it influences the decisions on information security investments. Liu et al. (2007) also conducted an empirical study on the G&L model to verify the relationship between the effects of an information security investment and the vulnerability level. Matsuura (2008) remarks that the G&L model derives its economic benefit from threat reduction, but concludes that this is not sufficient. Therefore Matsuura extended the G&L model to include a measure of productivity. Huang et al. (2008) have since extended the G&L model to include a risk-averse decision maker instead of a risk-neutral decision maker and adopted the expected utility theory. They have modelled the relationship between potential loss, the extent of risk aversion and the effectiveness of an information security investment. The majority of the work done seems to concentrate on how much to invest in information security. However, several important shortcomings still exist.

Recommendations drawn from the reviewed literature

The problem with the current body of knowledge is that it does not provide or recommend a set of requirements that decision makers have to consider when they develop their budgeting models. Requirements can act as a bridge in attempting to solve the problem of optimal resource allocation for information security. Furthermore, decision makers need to provide evidence of the success of their information security spending. Due to the difficulty in establishing the monetary value of information security benefits, requirements can also be used to act as the measure of success or failure of models for the allocation of resources. Requirements elicitation is therefore an acceptable departure point in the attempt to find solutions to the optimal and effective allocation of funds for information security.

3 Requirements

The need for efficient and effective budgeting and spending on information security is driven by a number of different high-level requirements, ranging from technological to

strategic issues. The elicitation of requirements for preparing an information security budget as proposed in this unit is structured as follows:

3.1 Requirements gleaned from existing approaches
3.2 Additional requirements

3.1 Requirements gleaned from existing approaches

The following list of requirements were identified from literature as referenced in this unit:

• Information security should be viewed as a multi-disciplinary field and therefore the budget should reflect implementation issues across the spectrum of people, process and technology.

• The budget should reflect implementation issues on the defence as well as attack side, i.e. proactive versus reactive.

• Careful consideration should be given to striking a balance between following a "standard-of-due-care" approach and following an approach based on risk assessment.

• An information security budget should address more than merely regulatory and standards compliance. An information security budget should be based on assumptions clearly communicated to senior management, with specific reference to the % coverage of vulnerability exposure as well as the % acceptable risk levels.

3.2 Additional Requirements

The authors of the material in hand have identified the following additional requirements to be considered when preparing a budget for information security:

- Taking cognisance of the three organisational levels
- Compiling and using a well-defined Information Security Architecture
- Other non-functional requirements

3.2.1 Taking cognisance of the three organisational levels

Cognisance has to be taken of the three well-known organisational levels, namely strategic, tactical and operational. These levels are to be used as framework for organising the proposed requirements:

a. Strategic Level

On the strategic level, the budget for information security should be aligned with the vision and mission statement of the organisation, the business goals, legal obligations, overall risk appetite and policy statements. Any money spent should be in direct support of realistic and reachable business goals and priorities of the organisation. The business

goals are derived from the vision, mission and values that are translated into the critical success factors of the organisation. This ensures that information security programmes are tightly coupled to the overall business strategy. Legal obligations are stipulated in national and international regulatory requirements and laws. Organisations are forced to adhere to these or face prosecution if they do not. Industry related laws and regulations must also be taken into account. Policy documents may also confirm the intent of an organisation, for example to protect the privacy of third parties. A policy describes the specific steps that an organisation will take and expects its employees to adhere to these in order to reach the organisation's business goals.

b. Tactical Level

The tactical level includes risk analysis for the identification of threats; standards and any compliance requirements. Thus it plays an important role in identifying threats to the security of information assets. It plays a guiding role in deciding 'how much' to spend on 'what'. Butler (2003) identifies a number of shortcomings of risk analysis, such as that exact investment decisions have to be made based on 'guesstimated' information. Compliance with international standards also influences the spending on information security. Many countries have equivalent standards on national level that reflect ISO/IEC 27002, such as the British Standard BS ISO/IEC 27002:2005 and the AS/NZS ISO/IEC 17799:2006 standard in New Zealand and Australia.

c. Operational Level

On the operational level, both operational and technological requirements need to be considered. Operational requirements include aspects such as affordability of manpower, resources, optimal protection levels and feasibility. Furthermore, the operational level includes administrative requirements referring to guiding the user's actions to meet business goals and objectives as specified on the strategic level. Technological requirements include both ICT infrastructure components such as controls on the hardware and software levels. When selecting controls, identification of an optimal mix of controls is of vital importance.

Compiling and using a well-defined Information Security Architecture

Eloff and Eloff (2005) proposed a number of requirements for the establishment of an information security architecture. These requirements – originally defined for developing information security architecture – can also be translated into requirements for information security budgets. The requirements state that information security architecture should:

I. **be holistic and encompassing**: The budget for information security should indeed be holistic and refer to the full spectrum of controls to be implemented. The

requirement of holism involves the inclusion of all aspects when budgeting for security. the budget should not focus on isolated aspects but on all aspects.

II. **make suggestions on how different controls can be synchronised and integrated to achieve maximum effect**: Very few organisations today spend enough time on the synchronisation and integration of controls, resulting in a potential over expenditure and duplication of controls. The synchronisation and integration of controls in most cases are organisation specific.

III. **include a comprehensive approach to information security risk management**: The relationship between a comprehensive approach towards risk management and the information security budget is self explanatory as the budget for information security should very clearly indicate how much risk mitigation is planned for, as well as the acceptable risk that the organisation will endure.

IV. **be measurable to demonstrate adherence to the requirements as set out**: Research has shown that it is somehow difficult to establish the monetary value of information security controls and of the benefits derived. Despite these difficulties, the results should be expressed in monetary terms.

Other non-functional requirements

Non-functional requirements are viewed as those that impose constraints on the compilation of the budget for information security. Dlamini et al. (2009), suggest the following high-level non-functional requirements:

• **Flexibility**: This requirement recognises the fact that organisations are different and that they exist in different sectors. One prescribed solution regarding information security controls will not satisfy the requirements of all organisations.

• **Cost effectiveness:** Organisations must be able to identify and implement those controls that will protect their information resources in the most cost effective way. Implementing all the controls may be a matter of "overkill", thus just "enough" should be implemented. Lastly, the existing and current information security budget must not be ignored as a valuable input into future budget definitions. The existing budget will also shape where recurring costs must be budgeted for, e.g. licensing fees on information security tools, hardware upgrades on information security technology.

Self Assessment Exercise

What are the requirements for the establishment of an information security architecture?

4.0 Conclusion

The entire business landscape finds itself on the verge of a recession because of ongoing global economic turmoil. Thus, there is a heightened need to minimise and mitigate

business risk and scrutinise information spending while ensuring compliance with regulatory mandates. This calls for decision makers to become vigilant in their spending and move towards an optimised information security investment.

5.0 Summary

This unit highlights the need for efficient and effective budgeting and spending on information security. It emphasizes a number of different high-level requirements, ranging from technological to strategic issues. The lists of requirements were identified such as the need for Information security to be viewed as a multi-disciplinary discipline with proactive and reactive measures bearing in mind the budget implication, with specific reference to the coverage of vulnerability exposure as well as the acceptable risk levels.

6.0 Tutor Marked Assignment

Discuss the relevance of information economics as a field of security

7.0 References/ Further Reading

Chapman, G. (2009) Cybercrime losses top $US1 trillion. Available online at: http://www.australianit.news.com.au/story/0,24897,24997483- 24169,00.html, accessed on 19 February 2009.

Goetz, E. and Johnson, M.E. (2006) Embedding Information Security Risk Management into the Extended Enterprise: An Executive Workshop, *MacNamee Center for Digital Strategies*, Tuck School of Business at Dartmouth University, USA. Available online at http://mba.tuck.dartmouth.edu/digital/Programs/CorporateEvents/CIO_RiskManage/Overview.pdf, accessed on 18 February 2009.

Huang, C.D., Hu, Q. and Behara, R.S. (2006) Economics of Information Security Investment in the Case of Simultaneous Attacks, *The Fifth Workshop on the Economics of Information Security (WEIS 2006)*, 26-28 January 2006, Robinson College, University of Cambridge, England.

Huang, C.D., Hu, Q. and Behara, R.S. (2006) Economics of Information Security Investment in the Case of Simultaneous Attacks, *The Fifth Workshop on the Economics of Information Security (WEIS 2006)*, 26-28 January 2006, Robinson College, University of Cambridge, England.

Liu, W., Tanaka, H. and Matsuura, K. (2007) Empirical-Analysis Methodology for Information-Security Investment and Its Application to Reliable Survey of Japanese Firms, Regular Paper, *IPSJ Digital Courier*, 3: 585 – 599.

Matsuura, K. (2008) Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model, *The Seventh Workshop on the Economics of Information Security*, 25-28 June 2008, Hanover, USA.

Srinidhi, B., Yan, J. and Tayi, G.K. (2008) Firm-level Resource Allocation to Information Security in the Presence of Financial Distress, *Working paper Series 2008-17*, School of Economic Sciences, Washington State University, USA. Available online at www.ses.wsu.edu/PDFFiles/WorkingPapers/Yan/Srinidhi_Yan_GiriJune 2008MISQ.pdf, accessed on 09 February 2009.

Su, X. (2006) An Overview of Economic Approaches to Information Security Management, Technical Report TR-CTIT-06-30, *Centre for Telematics and Information Technology*, University of Twente, Information Systems Group, Enschede, ISSN 1381 – 3625, Netherlands.

Tanaka, H., Matsuura, K. and Sudoh, O. (2005) Vulnerability and Information Security Investment: An Empirical Analysis of e-local Government in Japan, *Journal of Accounting and Public Policy*, Elsevier, 2005(24): 37-59.

Wang, Z. and Song, H. (2008) Towards an optimal information security investment strategy, *IEEE Conference on Networking, Sensing and Control 2008*, April 6 – 8, 2008, pp. 756 – 761.

Willemson, J. (2006) On the Gordon and Loeb Model for Information Security Investment, presented at *The Fifth Workshop on the Economics of Information Security* (WEIS 2006), University of Cambridge, UK, 26- 28 June 2006. Available online at http://www.ut.ee/~jan/publ/economics.ps, accessed on27 November 2007.