Internet and Information Security

Introduction

As organisations continue to use the Internet to carry out business processes, so does the security risks growing in accordance with it.

- Today, many organizations provide network access to their business partners, suppliers, customers and mobile employees, which give opportunities for people with bad intention to commit crimes such as Denial of Service Attack, Virus, Hacking and ID theft.

- A complete security program that includes round the clock management and monitoring, real-time security intelligence, global infrastructure as well as a staff of security experts working round the clock is the key to keeping pace with today's increasingly complex network security threats.

Learning Outcomes

For many organizations, the source of their competitive advantage is now based on the information which they use. A major concern, therefore, is the plurality of threats to such information.

This course will examine, in detail, those areas which are central to the task of managing security in the organizational context.

Underpinning the course is a socio-technical view of information security. Hence, rather than viewing security as a purely technical concern, **the course emphasizes the need to also consider the social context in which the technology is located.**

Learning Outcomes

There will be an in-depth examination of topics in the management of information technology security including:

- Access control systems and methodology
- Business continuity and disaster recovery planning
- Legal issues in information system security
- Ethics
- Computer operations security
- Physical security
- Security architecture and models

We will discuss security using current standards and models as well as cultural and behavioral issues.

Learning Outcomes

- The Information Security Governance and Risk Management domain entails the identification of an organization’s information assets and the development, documentation, implementation, and updating of policies, standards, procedures, and guidelines that ensure confidentiality, integrity, and availability.

- Management tools such as data classification, risk assessment, and risk analysis are used to identify threats, classify assets, and to rate their vulnerabilities so that effective security measures and controls can be implemented.

Expected to understand

- The student is expected to understand
  - the planning, organization, roles, and responsibilities of individuals in identifying and securing organization’s information assets;
  - the development and use of policies stating management’s views and position on particular topics and the use of guidelines, standards, and procedures to support the policies;
  - security training to make employees aware of the importance of information security, its significance, and the specific security-related requirements relative to their position;
  - the importance of confidentiality, proprietary, and private information; third party management and service level agreements related to information security;
  - employment agreements, employee hiring and termination practices, and risk management practices, and tools to identify, rate, and reduce the risk to specific resources.

Topics

- Information Security Concept
- Information Security Management
- Information Security Governance
- Information Classification
- Security Risk Management

Seven Types of Systems Security

- **Computer Security** focus on ensuring the availability and correct operation of a computer system without concern for information stored or processed by a computer E.g. Psd security, **Left out Integrity & confidentiality**

- **Network Security** consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources

- **Information Security** is concerned with **CIA** of data regardless of the form the data may take i.e: electronic, print

- **Internet Security -** is a branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems.

Seven Types of Systems Security

- **Cyber Security – Is concerned with securing the cyber space -** Strengthening the security and resilience of cyberspace and the interdependent network of IT infrastructures such as Internet, telecommunications networks

- **Physical Security -** an attacker might be able to simply enter the building and steal a laptop, paper documentation, flash drive, or disk from a server and walk right out with the system and the data on it.

- **Human Security** - Social Engineering method to steal information. users will click on links that are really malicious code, send sensitive information via unprotected methods, divulge passwords, write secure information down and post it in conspicuous places, reveal sensitive information over social media, and a veritable horror show of other such compromising behaviors.

Network Security Management

- **Network Security Management is the process of designing a security policy that will help to enforce an organization's systems user (Most Difficult task)** from gaining unauthorised access.

- **Information Assurance** focuses on the reasons for assurance that information is protected and ensures business continuity process.

What is Network Security Management Continue

- To specify an organization's information protection requirements, access controls, and audit requirements.

- It involves the process of restoring the system back in the event of failure e.g. (power supply, hardware, software, etc)

- To render an essential service unavailable for a period of time is consider unacceptable. Eg, Ebay, Air traffic control systems and Amazon website

- The processes of defining a Plan, Strategy and Policies in line with (ISO 27001/2) standards then implement them to prevent and ensure protection against intrusion and other network crimes.

Value of Information/Data

- Information is a valuable asset in any organization, whether it's printed or written on paper, stored electronically or sent by mail or electronic means.
  E.g. Banks, Passport Office, License Office, Insurance

- As organizations invest in and become more dependent on information systems, the processes of gathering, managing, and utilizing data become more central to operational success.

- **Data is only as valuable as our ability to access and extract meaning from it; and we cannot extract meaning from it without organizing, storing, and analyzing it effectively.**

Value of Information/Data

- **In the context of ISO 27001 and ISO 27002, an asset is any tangible or intangible thing that has value to an organization.**

- The protection of information and the establishment of a security management system are applicable to all types of organization, regardless of their size or the nature of their business

- To effectively manage the threats and risks to an organization's information, you should establish an Information Security Management System (ISMS 27001)

Security Objectives

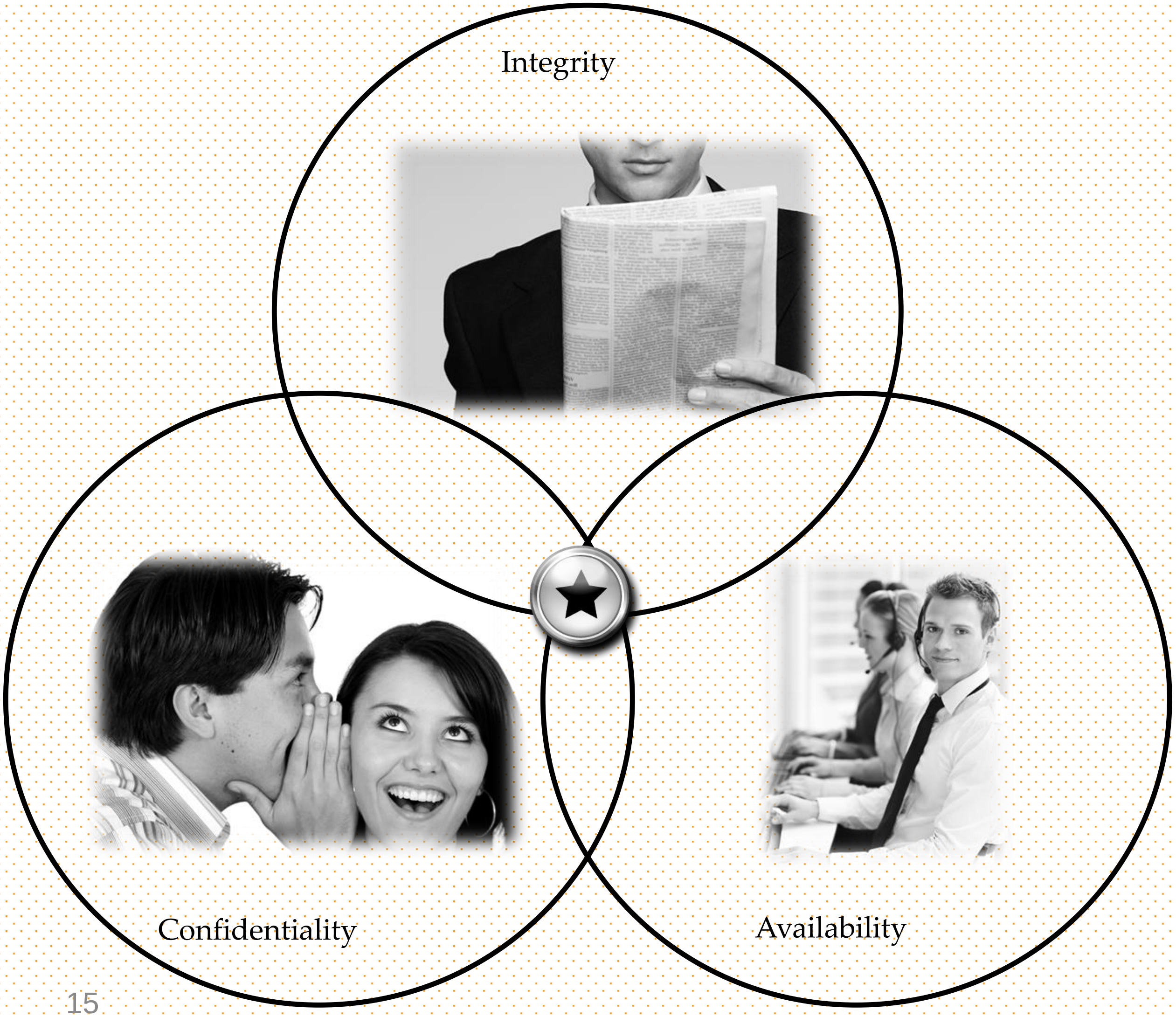
- **Confidentiality**
  - "Preserving authorized restriction on information **access** and **disclosure**, including means for protecting personal privacy and proprietary information." Confidentiality of ATM PIN Number, Account Information

- **Integrity**
  - "Guarding against improper information **modification** or **destruction**, and includes ensuring information nonrepudiation and authenticity." E.g ensure inf is correct

- **Availability**
  - "Ensuring **timely** and **reliable** access and use of information."
  - Eg, have my information whenever I need them

Security Goals

- C.I.A.



Importance of CIA Triad

Ensures:

- **Confidentiality, Integrity, Availability Triad**
- **Business Continuity Planning** -"identifies an organization's exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery for the organization, while maintaining competitive advantage and value system integrity”.
- **Business Process Reengineering** - is the analysis and design of workflows and processes . A logically related tasks performed to achieve a defined business outcome.
- **Information Assurance** - the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes.

CIA Triad A Security Model

- The confidentiality, integrity, and availability triad Three of the primary concepts in information security are confidentiality, integrity, and availability, commonly known as the confidentiality, integrity, and availability (CIA) triad

- The CIA triad gives us a model by which we can think about and discuss security concepts, and tends to be very focused on security, as it pertains to data.

Network Security Issues

- Networked systems and the sensitive information they contain can be compromised despite an administrator's best efforts.

- Administrators need a clear and comprehensive set of security practices that are easy to find and follow.

- Security Improvement addresses an important but narrowly defined problem in network security. It provides guidance to help organizations improve the security of their networked computer systems.

Policy

- Can be considered as a "Statement of Intent" or a "Commitment". For that reason at least, the decision makers can be held accountable for their policy after it has been authorized.

- **Policy merely guides actions toward those that are most likely to achieve a desired outcome.**

The term may be applicable to:

- Government sectors – MDA, Hospital, Schools, Banks, Insurance Companies (SIC)
- Private sector organizations – Banks, Insurance Companies, School, Law firms
- Individuals – Sole Proprietary and or SMEs

We will discuss more about Policies later

Authenticity

- Authenticity allows us to talk about the proper attribution as to the owner or creator of the data in question.
  - For example, if we send an e-mail message that is altered so as to appear to have come from a different e-mail address than the one from which it was actually sent, we would be violating the authenticity of the e-mail.
  - Authenticity can be enforced through the use of digital signatures,

Security from Business Perspective

Two types of Security from Businesses Perspective

- **Service Orinted** – e.g. Hospital, Schools, CSIR, Universities, Police, Fire Services
- **Profit Oriented** – Banks, Air Travel Org, Insurance Companies etc

Security Risks

- Security risks are growing in accordance as organisations continue to use the Internet to carry out business processes.

- Organizations provide network access to their business partners, suppliers, customers and mobile employees (e.g. Banks and Air Travel KLM, Virgin), which give opportunities for people with bad intention to commit crimes such as:

- Denial of Service Attack, Virus, Hacking and ID theft, Sabotage, Industrial espionage

- (SWOT Analysis) Strength, Weaknesses, Opportunities & Treat

Threat Intelligence

W32.Flamer is a worm that may attempt to spread when it receives instructions from a remote attacker. It also opens a back door and may steal information from the compromised computer.

- Impact - (Loss of Data) – Confidentiality, Availability and Integrity

- Discovered: May 28, 2012 Updated: June 5, 2012 3:20:22 PM
- Also Known As: WORM_FLAMER.A [Trend]

Flamer Threat

Flamer Threat

- On May 28th Symantec released its analysis of a threat called Flamer. Flamer is a highly sophisticated threat, using multiple components that cleverly conceal its malicious functionality
- The complexity of the code within this threat is commensurate with that seen in Stuxnet and Duqu, arguably the two most complex pieces of malware we have analyzed to date. Symantec Threat Write-up: W32.Flamer

CVE References:

CVE-2010-2568, CVE-2010-2729

http://www.symantec.com/security_response/writeup.jsp?docid=2012-052811-0308-99

Threat Intelligence

Defining when we are insecure is a much easier task, and we can quickly list a number of items that would put us in this state:

- Not patching our systems or not patching quickly enough
- Using weak passwords such as “password” or “12345678”
- Downloading infected programs from the Internet
- Opening dangerous e-mail attachments from unknown senders
- Using wireless networks without encryption that can be monitored by anyone

Threat Intelligence
Industrial Espionage

Stuxnet is a computer worm discovered in June 2010.

- Stuxnet initially spreads via Microsoft Windows, and targets Siemens industrial software and equipment.
- While it is not the first time that hackers have targeted industrial systems, it is the first discovered malware that spies on and subverts industrial systems, and the first to include a programmable logic controller (PLC) root kit.
- The worm initially spreads indiscriminately, but includes a highly specialized malware payload that is designed to target only Siemens supervisory control and data acquisition (SCADA) systems that are configured to control and monitor specific industrial processes.
- Stuxnet infects PLCs by subverting the Step-7 software application that is used to reprogram these devices.

Threat Intelligence
Industrial Espionage

- Stuxnet targeted five Iranian organizations suspected to be uranium enrichment infrastructure
- Symantec noted in August 2010 that 60% of the infected computers worldwide were in Iran
- On 1 June 2012, an article in The New York Times said that Stuxnet is part of a U.S. and Israeli intelligence operation called "Operation Olympic Games",
- started under President George W. Bush and expanded under President Barack Obama.
- http://en.wikipedia.org/wiki/Stuxnet

Threat Intelligence
Malware Duqu

Duqu - computer worm discovered on 1 September 2011, thought to be related to the Stuxnet worm.

- The Laboratory of Cryptography and System Security (CrySyS Lab) of the Budapest University of Technology and Economics in Hungary discovered the threat, analysed the malware, and wrote a 60-page report naming the threat Duqu.

- Duqu got its name from the prefix "~DQ" it gives to the names of files it creates.

Threat Intelligence
Malware Duqu

- Duqu malware is a variety of software components that together provide services to the attackers.
- Currently this includes information stealing capabilities and in the background, kernel drivers and injection tools.

- Part of this malware is written in unknown high level programming language, dubbed "Duqu framework". It is not C++, Python, Ada, Lua and many other checked languages. However, recent evidence suggests that Duqu may have been written in Object Oriented C (OO C) and compiled in Microsoft Visual Studio 2008.

- Duqu flaw is the flaw in Microsoft Windows that is used in malicious files to execute malware components of Duqu.

- Currently one flaw is known, a TTF related problem in win32k.sys.

http://en.wikipedia.org/wiki/Duqu

Threat Intelligence Malware Duqu

Spyware - software that monitors a user's computers

- Spyware is a type of malware (malicious software) installed on computers that collects information about users without their knowledge.

- The presence of spyware is typically hidden from the user and can be difficult to detect.

- Some spyware, such as keyloggers may be installed by the owner of a shared, corporate, or public computer intentionally in order to monitor users.

- Spyware can collect almost any type of data, including personal information like Internet surfing habits, user logins, and bank or credit account information.

Threat Intelligence
Malware Duqu

- Spyware can also interfere with user control of a computer by installing additional software or redirecting Web browsers.
- Some spyware can change computer settings, which can result in slow Internet connection speeds
- Sometimes, spyware is included along with genuine software, and may come from an official software vendor.
- Running anti-spyware software has become a widely recognized element of computer security practices for computers, especially those running Microsoft Windows.
- A number of jurisdictions have passed anti-spyware laws, which usually target any software that is surreptitiously installed to control a user's computer.

http://en.wikipedia.org/wiki/Spyware

Industrial Espionage.

Former Pentagon analyst: China has backdoors to 80% of telecoms

- **Summary:** A former Pentagon analyst reports the Chinese government has "pervasive access" to about 80 percent of the world's communications, and it is looking currently to nail down the remaining 20 percent.

- Chinese companies Huawei and ZTE Corporation are reportedly to blame for the industrial espionage.
  - July 14, 2012 -- Updated 18:43

http://www.zdnet.com/former-pentagon-analyst-china-has-backdoors-to-80-of-telecoms-7000000908/

Security Implementation Principles

- **Confidentiality, Integrity, Availability**
- **Need-to-know**
  - Users should only have access to information (or systems) that enable them to perform their assigned job functions.
- **Least privilege**
  - Users should only have sufficient access privilege that allow them to perform their assigned work.
- **Separation of duties**
  - No person should be responsible for completing a task involving sensitive, valuable or critical information from the beginning to end.
  - No single person should be responsible for approving his/her own work.

The Need for Security Management

Although organizations may have established strong perimeter security, it is only a first line of defence.

To effectively safeguard critical information:

- Integrate the latest security enabled devices and software's
- A complete security program that includes around the clock management, training and monitoring
- Establish real-time security intelligence and Global infrastructure. For compatibility purposes
- Staff of security experts working round the clock (the key to keeping pace with today's increasingly complex network security threats)