**Professional Practices in Information Technology**

Hand Book



COMSATS Institute of Information Technology

(Virtual Campus)

Islamabad, Pakistan

Lecture No. 1

Professional Practices in IT

**1.1 Introduction**

The objective of the course is to make students aware of their professional responsibilities when they will work in IT sector. The course will teach students about the historical, social, ethical, economical and professional issues related to IT profession.

* **Information Technology**

IT (information technology) is a term that encompasses all forms of technology used to create, store, exchange, and use information in its various forms (business data, voice conversations, still images, motion pictures, multimedia presentations, and other forms, including those not yet conceived). It's a convenient term for including both telephony and computer technology in the same word. It is the technology that is driving what has often been called "the information revolution."

More formal definition of information technology is: *“Information Technology (IT) describes any technology that helps to produce, manipulate, store, communicate, and/or disseminate information, Part 1: Computer Technology, Part 2: Communication Technology”.*

In a business context, the Information Technology Association of America has defined information technology as "*the study, design, development, application, implementation, support or management of computer-based information systems".* The responsibilities of those working in the field include network administration, software development and installation, and the planning and management of an organization's technology life cycle, by which hardware and software is maintained, upgraded and replaced.

* **How is IT being used in Education?**

Almost 99% universities in Pakistan have internet access. Majority of university students own their own computer. 80% of students use the internet for 4 or more hours per week. ½ of professors in universities require students to use email in their classes. Distance Learning such as this is a prime example of usage of IT in education.

* **Health: High Tech for Wellness**

Telemedicine is medical care via telecommunications lets doctors treat patients from far away. 3D Computer models allow accurate tumor location inside a skull. Robots permit precise microsurgery. Handheld computers allow patients to measure blood sugar. Medical implants allow stroke patients to directly control computers to talk for them. Health websites provide medical information.

* **Money: Cashless Society**

Definition: Virtual means something that is created, simulated, or carried on by means of a computer or a computer network. For example, virtual airline tickets, virtual money, online bill paying, PayPal, electronic payroll deposit, micropayments for online music etc.

* **Leisure: InfoTech in Entertainment & the Arts**

Information technology is also used for entertainment and arts. For example, video games, downloading, movies, music, ebooks. Most movies use computer animation and digital editing.

* **Jobs & Careers**

Information technology helps office careers like budget, payroll, letter-writing, email. Teaching career for automated grading systems, emailing, distance teaching. Fashion career for sales/inventory control systems, ordering, personnel. Information technology is also useful for job-hunting, word processor to create resumes; post resumes online, online job searches.

* **The Telephone Grows Up**

The first cell phone call was made in 1973. In 2006, Nokia estimates 2 billion mobile phone subscribers. Today’s cellphones are mobiles; these can take and send pictures, connect to the internet, can send and receive text messages.

**1.2 Internet, World Wide Web, & Cyberspace**

* **World Wide Web**

It is the multimedia part of the internet. It is an interconnected system of servers that support specially formatted documents in multimedia form. It includes text, still images, moving images, sound. These things are responsible for the growth and popularity of the internet.

* **Cyberspace**

Term coined by William Gibson in Neuromancer (1984). They described it as a futuristic computer network where people “plugged” into directly with their brains.

Now through means like:

The web

Chat rooms

Online diaries (blogs)

The wired and wireless communications world

**1.3 Five Computer Types**

Five main types of computers are:

* Supercomputers
* Mainframe Computers
* Workstations
* Microcomputers
* Microcontrollers
* **Supercomputers**

Supercomputers are priced from $1 million to $350 million. These are high-capacity machines with thousands of processors. Supercomputers include multi-user systems.

* **Mainframe Computers**

Until late 1960’s, the only computer available were mainframe computers. These computers cost $5,000 - $5 million. These were also multi-user systems; accessed using a terminal. The terminals only have a keyboard and monitor; can’t be used alone.

* **Workstations**

Workstations were introduced in early 1980s. These were expensive, powerful personal computers. Used for scientific, mathematical, engineering, computer-aided design (CAD), computer-aided manufacturing (CAM). These were less-expensive and an alternative to mainframes.

* **Microcomputers**

Microcomputers are personal computers that cost Rs. 20,000 to Rs. 200,000. These are used either as stand-alone or in a network. Types include: desktop, tower, notebooks, or Personal Digital Assistants (PDAs).

* **Microcontrollers**

Microcontrollers are also called embedded computers. These are tiny, specialized microprocessors inside appliances and automobiles. They are in: microwaves, programmable ovens, blood-pressure monitors, air bag sensors, vibration sensors, MP3 players, digital cameras, e-pliances, keyboards, car engine controllers, etc.

**1.4 Servers**

Servers are central computers. Servers may be from computer types. “Server” describes a function; hold data (databases) and programs, connect to and supply services for clients. Clients are other computers like PCs, workstations, other devices

* **Convergence, Portability, & Personalization**

Convergence is the combination of computers, consumer electronics, entertainment and mass media.

Portability is collaboration software that allows people to share anything instantly. Help people to enhance the information as they forward it.

**1.5 Future of Information Technology**

3 directions of Computer Development are Miniaturization, Speed and Affordability.

3 directions of Communications Development are Connectivity, Interactivity and Multimedia.

Lecture No. 2  
Professionalism

**2.1 Professionalism Takes More than Knowledge**

## “Professionalism is a way of thinking and living rather than an accumulation of learning.” Think: What does it take to be a doctor? It’s not just by going to medical school.

# A profession isn’t just what you do, it’s who you are. We say that somebody “is” a doctor. Here, “doctor” is a noun (“Doctoring the books” is something different!). Likewise, we don’t just “engineer” (verb), we also are engineers (noun).

* **A profession is who you are, not a contract**

## “Shame on the engineer who regards their professional function as a business transaction to be judged by the question: ‘Just what do I get out of it?’”

## What “professions” have a reputation for being self-centered and selfish?

* **Life as a professional: activities**

## You perform “professional activity of a type carrying high individual responsibility, requiring application of special skills to activities that are predominantly intellectual and varied rather than routine and normal.”

## How are an engineer’s activities “varied”?

## **Life as a professional: motivation**

## “Motivation for service takes first place over consideration of reward.”

# **Life as a professional: joy and pride**

## “Motivation … implies joy and pride in the work to be done, and self-imposed standards.” If you don’t take joy and pride in computer science, then you should look for another line of work. Companies and customers are also entitled to impose (secondary) standards of excellence.

# **Life as a professional: social duty**

## You have a “social duty, fulfilled through guarding the ideals and standards of the profession, by advancing it …, by sharing advances …, by rendering gratuitous public service, all as a return to society.” “Giving back” to society

**2.2 Four traits of a professional**

## Varied activities requiring special skills

## Society-centric motivation

## Personal standards of excellence

## Giving back to society

* **When you put many professionals together, what do you have?**

## A profession isn’t just defined by who you are. A profession is also something you are part of. “Most professional software engineers adopt an institutional view of the organizations of the profession: they perceive them as bodies representing the profession and therefore deserving, even requiring, the loyalty of each software engineer as an expression of his identity as a professional software engineer.”

* **Part of being a professional is behaving ethically**

## “Ethics means something more than ‘law’ and ‘morals’; it carries an additional connotation of ‘rightness’.”

## Breaking the law: can earn a fine or jail time

## Breaking a moral: can ruin your reputation

## Breaking an ethic: can ruin your conscience

## It’s possible to break all three, simultaneously!

# **Trait # 1 of a professional: Seriousness**

## Serious about job

## The job is only a job. A means to an end

# **Trait # 2 of a professional: Wanting to do better**

## Exhibit a never-ending quest to improve their performance in every variable, every project, every relationship, and every detail.

# **Trait # 3 of a professional: Dealing with the Unexpected**

## Stuff happens, things change, and the true professional rises to the occasion

# **Trait # 4 of a professional: Communication Skills**

## Clear

## Concise

## Confident

# **Trait # 5 of a professional: Enthusiasm**

## Attitude is everything. Those who exhibit enthusiasm for what they do and greet each day with a positive attitude inevitably become a leader

# **Trait # 6 of a professional: Helpfulness**

## Understand that real success in the workplace requires teamwork

## Always ready to lend a hand

## Make a suggestion

## Offer a compliment when it’s deserved

# **Trait # 7 of a professional: Taking the Initiative**

## Takes the initiative to get things done

# **Trait # 8 of a professional: Cool under Pressure**

## Level headed and calm

## Cheerful demeanor-even under stressful times

# **Trait # 9 of a professional: Remains Focused**

## Stay focused on the task at hand and the goal ahead

## Navigate through obstacles or setbacks but never lose sight of where they headed

# **Trait # 10 of a professional: Don’t Follow, Lead**

## True Professionals aren’t faint of heart

## Analyze the situation and willing to take new paths and try new solutions

## That’s why they call it LEADERSHIP!

* **Laws vs Morals vs Ethics**
* Speeding on Motorway

### Illegal, moral (“everyone” does it), maybe ethical

## Speeding within city

Illegal, immoral, unethical

## What might a software engineer do that is…

Illegal, immoral, unethical ?

Legal, immoral, unethical ?

Legal, moral, unethical ?

**2.3 IEEE Code of Ethics: Actions**

## 1. PUBLIC - Software engineers shall act consistently with the public interest.

## 2. CLIENT AND EMPLOYER - Software engineers shall act in a manner that is in the best interests of their client and employer consistent with the public interest.

# **IEEE Code of Ethics: Products**

## 3. PRODUCT - Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.

# **IEEE Code of Ethics: Hierarchy**

## 4. JUDGMENT - Software engineers shall maintain integrity and independence in their professional judgment.

## 5. MANAGEMENT - Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.

# **IEEE Code of Ethics: Peers**

## 6. PROFESSION - Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.

## 7. COLLEAGUES - Software engineers shall be fair to and supportive of their colleagues.

# **IEEE Code of Ethics: Self**

## 8. SELF - Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.

**2.4 8 Principles of IEEE Code of Ethics**

## Act in public interest

## Act in interest of clients and employers

## Produce quality products

## Maintain independent judgment

## Manage ethically

## Protect integrity of profession

## Support colleagues

## Pursue lifelong learning

* **Scenario #1**

## You are the owner of a software engineering company. Your employees (engineers) want you to pay for them to attend training.

## How would you respond in a way that is legal, moral, and ethical?

* **Scenario #2**

## You are the owner of a software engineering company. Your employees (engineers) want you to let them do pro bono work for a local non-profit organization on company time.

## How would you respond in a way that is legal, moral, and ethical?

* **Scenario #3**

## You are the head of a computer science department at a university. Your boss (a “dean”) wants you to find a way to tweak your curriculum so undergrads are more likely to choose your department for their major.

## How would you respond in a way that is legal, moral, and ethical?

* **Scenario #4**

## You are a software engineer working at a large publicly-traded corporation, where a colleague invents a new kind of compiler. Your managers see it as a huge potential cash cow.

## How would you respond in a way that is legal, moral, and ethical?

* **Scenario #5**

## You are a software engineer at a company where management routinely encourages you and your colleagues to use pirated software.

## How would you respond in a way that is legal, moral, and ethical?

Lecture No. 3

Professional Ethics & Codes of Conduct

**3.1 Motivation for “Code of Ethics”**

## **Historical**

## Professional associations use mechanism to establish status as a profession. Regulate their membership and convince public that associate deserves to be self-regulated.

* **Self-regulation: one solution**

## Apply code of ethics

## Ethics review board

## Deter unethical behavior of members

* **Code of ethics**

## Lists possible violations

## Threaten sanctions for such violations

## Association of Computing Machinery (ACM)

### One of the two most important professional associations for computer scientists / IT professionals

### 1972: Code of Professional conduct and 1992: Code of Ethics and Professional Conduct.

### Difficulties implementing ethics review system

## 1972’s goal was “carrots and sticks”

## 1992’s goal: major shift towards socialization and education

## Clarifies professionals’ responsibility to society

* **Most important goal**

## Provides an aid to individual decision making, presentation addresses nine different cases (with some overlap)

## Intellectual property

## Privacy

## Confidentiality

## Professional quality

## Fairness or discrimination

## Liability

## Software risks

## Conflicts of interest

## Unauthorized access to computer systems

**3.2 ACM Code of Ethics**

## General moral imperatives: “As an ACM member I will…”

## Contribute to society and human well-being.

## Avoid harm to others.

## Be honest and trustworthy.

## Be fair and take action not to discriminate.

## Honour property rights including copyrights and patents.

## Give proper credit for intellectual property.

## Respect the privacy of others.

## Honour confidentiality.

## Specific professional responsibilities: “As an ACM computing professional I will”:

## Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work.

## Acquire and maintain professional competence.

## Know and respect existing laws pertaining to professional work.

## Accept and provide appropriate professional review.

## Give comprehensive and thorough evaluations of computer system and their impacts, including analysis of possible risks.

## Honour contracts, agreements, and assigned responsibilities.

## Improve public understanding of computing and its consequences.

## Access computing and communication resources only when authorized to do so.

## Organization leadership imperatives: “As an ACM member and an organizational leader, I will:”

## Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities.

## Manage personnel and resources to design and build information systems that enhance the quality of working life.

## Acknowledge and support proper and authorized uses of an organization’s computing and communication resources.

## Ensure that users and those who will be affected by a design have their needs clearly articulated during the assessment and design of requirements; later the system must be validated to meet requirements.

## Articulate and support policies that protect the dignity of users and others affected by a computing system.

## Create opportunities for members of the organization to learn the principles and limitations of computer systems.

## Compliance with the Code: “As an ACM member, I will:”

## Uphold and promote the principles of this Code.

## Treat violations of this code as inconsistent with membership in the ACM.

* **Ethical decision making: Case 1**

## **Ali is a database programmer**

## Large statistical program needed by his company (actuarial requirements)

## Company programmers are encouraged to publicize their work

## **Ali has found himself stuck on a problem**

## Has persisted at this for several months

## His manager does not recognize complexity of problem.

## She insists job be completed in the few days.

## **Ali remembers:**

## Co-worker had given him source listings of their current work

## He also has an early version of commercial software developed at another company

## **Ali studies these programs**

## Sees two areas of code which could be directly incorporated into his own program

## He uses segments of code both from his coworker and from the commercial software

## He does not tell anyone or mention it in the documentation.

## He completes the project and turns it in a day ahead of time.

## How does the Code of Ethics help us understand this case?

* **Applying the code: Case 1**

## **This case highlights issues involving intellectual property**

## 1.6: “Give proper credit for intellectual property”

## Specifically, do not take credit for other’s ideas or work.

## **Property rights principle (1.5)**

## copyrights, patents, trade secrets, license agreements

## **Restrictions also ground in:**

## integrity (1.3)

## complying with existing laws (2.3)

## **Ali violated professional ethics in two areas:**

## Failure to give credit for another’s work

## Using code from a commercial package that (presumably) was copyrighted

## **If Ali only “looked” at co-worker’s source code:**

## Could he then write his own program and still have an obligation to give credit?

## **Yes:**

## He should have acknowledged credit in documentation.

## (Some professional discretion possible here, especially if intellectual material is trivial)

## **Use of commercial software code was also not appropriate:**

## Ali should have checked to determine whether or not company was authorized to use source code before using it.

## **In general:**

## Desirable to share and exchange intellectual materials

## But using bootlegged software is definitely a violation of code.

* **Ethical decision making: Case 2**

## Three years ago, Aisha started her own consulting business

## She is so successful she now has several people working for her.

## Have many clients.

## Includes work such as advising on network architectures, designing DBMSes, security.

## Presently designing a DBMS for the personnel office a medium-sized (100 person) company

## Aisha has involved client in design process

## Informs CEO, CTO and human resources head about system progress

## Now it is time to make decisions about the kind and degree of security to build into system.

## Aisha has described several options.

## Because of cost overruns, client has decided to opt for a less secure system.

## Aisha believes information they will store is extremely sensitive (performance evaluations, medical records for insurance claims, salaries, etc.)

## With weak security:

## Employees on workstations could figure out how to access this data.

## Online intruders would also have access

## Aisha feels strongly that system should be much more secure.

## She has tried to explain the risk.

## CEO, CTO and HR all agree that less security will do.

## What should Aisha so?

## Should she refuse to build the system as they request?

* **Applying the Code: Case 2**

## This case highlights issues involving privacy

## Principle 1.7 deals with privacy

## Principle 1.8 deals with confidentiality

## Code guidelines state that:

## “Computer professionals are obligated to preserve the integrity of data about individuals…”

## “… from unauthorized access or accidental disclosure to inappropriate individuals”

## Code also specifies for organizational leaders:

## Principle 3.5 (enhance personal dignity)

## Principle 3.4 (assess needs of all those affected by system)

## Company officials:

## Have an obligation to protect privacy of their employees.

## Therefore they should not accept inadequate security.

## Aisha’s first obligation:

## Attempt to educate company officials (implied by principle 2.7)

## If that fails, she needs to consider her contractual obligations (principle 2.6) in honouring assigned responsibilities.

## We don’t have Aisha’s contract, but she may have to choose between her contract and her obligation to honour privacy and security.

Lecture 04

Professional Ethics & Codes of Conduct

* **Ethical Decision Making: Case 3**

## Sana works in a large provincial agency dealing with alcoholism and drug abuse. Agency administers programs for individuals with alcohol and drug programs.

## Maintains a large database of information on clients who use agency services

## Some data files contain names and current addresses of clients.

## Sana has been asked to look at the track records of treatment programs.

## Reporting # of clients seen each month for past five years, length of client treatment, number of clients who return after program completion, criminal histories of clients.

## Sana has been given access to all files in the agency’s mainframe computer

## This data is needed to put together in the report.

## After assembling data:

## She downloads it to the computer in her office.

## The agency is pressuring her to finish report on the deadline.

## Sana decides she must work from home over the weekend.

## She copies data onto several disks and takes them home.

## After finishing report she leaves the disks at home and forgets about them.

* **Applying the Code: Case 3**

## This case resembles case 2, but raises several additional issues. Issues involving confidentiality

## Principle 1.7 deals with privacy

## Principle 1.8 deals with confidentiality

## Principle 2.8 also applies:

## Constraining access to authorized systems

## Principle 3.5:

## Organizational leaders have obligations to “verify systems are designed and implemented to protect personal privacy and enhance personal dignity”.

## Also Principle 3.3:

## (Appropriate and authorized uses of organization’s resources)

## Government agency should have had policies and procedures to protect identity of its clients

## Sana’s friends and relatives might accidentally discover files and inappropriate uses information.

## Note that the files Sana used did not need to have names or other information in the records.

## Agency should have removed identifying information from files Sana was allowed to use.

## If this happened, it wouldn’t have mattered that Sana copied files to her computer.

## Sana, unfortunately, was not attentive to ethical issues ahead of time.

* **Ethical decision making: Case 4**

## Computer Company is writing first part of an “efficient accounting system”.

## Will be used by government

## Expectation is that this will save taxpayers a considerable amount of money each year.

## Software engineer in charge of design assigns different parts of system to his staff.

## Reports, Internal Processing, User interface

## Manager is shown the system, and agrees it matches requirements. System is installed, but staff found the interface so difficult to use that their complaints are heard by upper-level management.

## Result of complaints:

## Upper-level management will not invest any more money in developing the new accounting system

## They go back to their original, more expensive system

* **Applying the Code: Case 4**

## This case highlights issues involving quality of professional work Code of Ethics advocates that:

## Professional strive to achieve the highest quality in both process and products (2.1)

## Principle 3.4: users and those affected by a system must have their needs clearly articulated

## Assumption in this case:

## Failure to deliver a quality product is directly attributable to failure to follow a quality process.

## Most likely the problems with interface could have been discovered in review process – peers or users (2.4)

## When harm results (in this case with taxpayers), failure to implement quality process clearly violates ethical behavior.

* **Ethical decision making: Case 5**

## Contractor is determining requirements for an employment agency.

## Client describes what is needed when displaying applications whose qualifications appear to match those for a particular job

## Client also further states that names of white applicants are to be displayed ahead of nonwhites

## Further states that names of male applicants are to be displayed ahead of female applicants

## Recall: ethical code asserts an ACM member will be “fair and take action not to discriminate”

* **Applying the Code: Case 5**

## This case highlights issues involving fairness and discrimination. In this case, system designer is asked to build a system that, it appears

## Will be used to favour white males and

## Discriminate against non-whites and females

## From this is would appear that:

## System designer should not do what he or she is told, plus

## Should also point out the problematic nature of what is being requested and ask client why this is being done

## Making the inquiry is consistent with 2.3, 2.5 and 4.1.

## If client answers that they plan to use information to favour white males, then:

## Computer professional should refuse to build the system as proposed.

## To go ahead and build the system would violate:

## 1.4 (fairness)

## 2.3 (respecting existing laws)

## It would also be inconsistent with:

## 1.1 (well-being)

## 1.2 (avoiding harm)

* **Ethical decision making: Case 6**

## A software development company has just produced a new software package.

## It incorporates new tax laws and prepares both individual and small business tax returns

## The president of the company knows that the program has a number of bugs

## He also believes the first firm to put this kind of software on the market is likely to capture the largest market share.

## The company widely advertises the package.

## When the product is shipped, it includes a disclaimer of responsibility for errors resulting from the use of the program.

## The company expects it will receive a number of complaints, queries, and suggestions for modification. The company plans to use these to make changes and eventually issue updated, improved and debugged versions. The president argues that this is general industry policy:

## “Anyone who buys version 1.0 of a program knows this and will take proper precautions.”

## Because of bugs, a number of users filed incorrect tax returns and were penalized by Rev Canada.

* **Applying the Code: Case 6**

## This case highlights issues involving legal liability for unreliable code. Software Company (and president in particular) violated several principles in the ACM code of ethics. Since he was aware of bugs in the product, he did not strive to achieve the highest quality (Principle 2.1). By failing to inform consumers about bugs to system, principle 2.5 was violated. Here the risks to users are so great they have to pay penalties for mistakes which result from the program.

## By law companies can make disclaimers only when they are in “good conscience” (Disclaimer does not meet legal test, violated principle 2.3)

## President also violates Principle 3.1

* **Ethical decision making: Case 7**

## Small Software Company is working on an integrated inventory control system

## Very large national shoe manufacturer

## System gathers sales data daily from stores across Canada

## Data is used by following departments:

## Accounting

## Shipping

## Ordering

## Inventory functions are critical to the smooth operation of the system and the corporation.

## James is a quality assurance (QA) engineer with the software company

## He suspects the inventory functions of the system are not sufficiently tested

## However, they have passed all contracted tests.

## He is being pressured by his employers to sign off on the software. Legally he is only required to perform those tests which found their way into the contract. However, his considerable experience in software testing leads him to be concerned over risks of incorrect system behavior.

## Despite insisting, James’ company states:

## “We will go out of business if we do not deliver the software on time.”

## James replies:

## “If inventory subsystem fails, it will significantly harm our client and their employees.”

## If the potential failure were to threaten lives, it would be clear to James that he should refuse to sign off. However, given the reduced degree of threatened harm, James is faced by a difficult decision.

* **Applying the Code: Case 7**

## This case highlights issues involving software risks. Principle 1.2 stress responsibility of computing professional to avoid harm for others

## Principle 1.1 requires concern for human well-being

## Principle 1.3 mandates professional integrity

## Principle 2.1 defines quality as an ethical responsibility

## These principles may conflict with agreements and commitments of an employee to the employer and client.

## The ethical imperatives of the code suggest that:

## James should not deliver a product he believes to be inferior

## Nor should he mislead the client about the quality of the product (1.3)

## He should continue to test, and has been told of the financial repercussions of not delivering the system.

## At the very least, the client should be informed of his reservations.

* **Ethical decision making: Case 8**

## A software consultant is negotiating a contract with a local municipality, designing their traffic control system (TCS). She recommends they select the TCS system out of several available systems on the market. The consultant fails to mention that she is a major stockholder of the company producing TCS software.

* **Applying the Code: Case 8**

## This case highlights issues involving conflicts of interest. Principle 2.5: computer professionals must “strive to be perceptive, thorough and objective when evaluating, recommending and presenting system descriptions and alternatives.” Principle 1.3: implies a computer professional must be honest about “any circumstances that might lead to conflicts of interest”.

## IT professionals have special skills

## It is their responsibility to ensure clients are fully aware of the options.

## Also their responsibility to ensure professional recommendations is not modified for personal gain.

* **Ethical decision making: Case 9**

## Hugo is working on a project for his computer science course. Instructor has allotted a fix amount of computer time for the project.

## This time is enforced by the computer system.

## Hugo runs out of time, but has not yet finished the project. Instructor cannot be reached. Hugo worked last year as a co-op programmer in the department. He is very familiar with procedures used to increase time allocations to accounts. Using what he learned last year, he is able to access the master account. Then he gives himself additional time. He now completes his project.

* **Applying the code: Case 9**

## Principle 1.5 (property rights) has been violated. Principle 2.8: specifies that ACM members should “access communication resources only when authorized to do so”. By violating 2.8, Hugo is also violating Principle 2.3 (“know and respect existing laws”). As a student member of the ACM, Hugo must follow the code of ethic even if he does not consider himself a computing professional.

**3.3 Nine Cases: Summary**

## Illustrate broad range of issues facing an IT professional.

## Code does not prescribe what an individual must do

## But it does identify some decisions as unacceptable.

## Ethical decision often involves balance amongst several factors.

## Computer professionals therefore have to choose amongst the conflicting principles.

## Goal is to ahead to the spirit as much as to the letter.

## All of the cases also portrayed individuals acting in constrained situations.

## Institutional environment usually influences ethical decisions.

## Such environments can either facilitate or constrain ethical behavior.

## Leadership roles set the tone.

## Some of the problems shown in the cases resulting from a lack of ethical leadership

* **Other applicable codes**

## Canadian Information Processing Society (CIPS):

## Code of Ethics & Standards of Conduct, http://www.cips.ca/about/ethics/english/ethics.pdf

## IEEE Computer Society & ACM:

## Software Engineering Code of Ethics and Professional Practice, http://www.computer.org/computer/code-of-ethics.pdf

## Council of Professional Engineers

## Guideline on the Code of Ethics, http://www.ccpe.ca/e/files/guideline\_code\_with.pdf

Lecture 5 & 6  
Cyberethics

**5.1 What Is Cyberethics?**

## Cyberethics is the study of moral, legal, and social issues involving cybertechnology. It examines the impact that cybertechnology has for our social, legal, and moral systems. It also evaluates the social policies and laws that have been framed in response to issues generated by the development and use of cybertechnology. Hence, there is a reciprocal relationship here.

* **What Is Cyber technology?**

## Cybertechnology refers to a wide range of computing and communications devices – from standalone computers, to "connected" or networked computing and communications technologies, to the Internet istself.

## Cybertechnologies include: hand-held devices (such as Palm Pilots), personal computers (desktops and laptops), mainframe computers, and so forth.

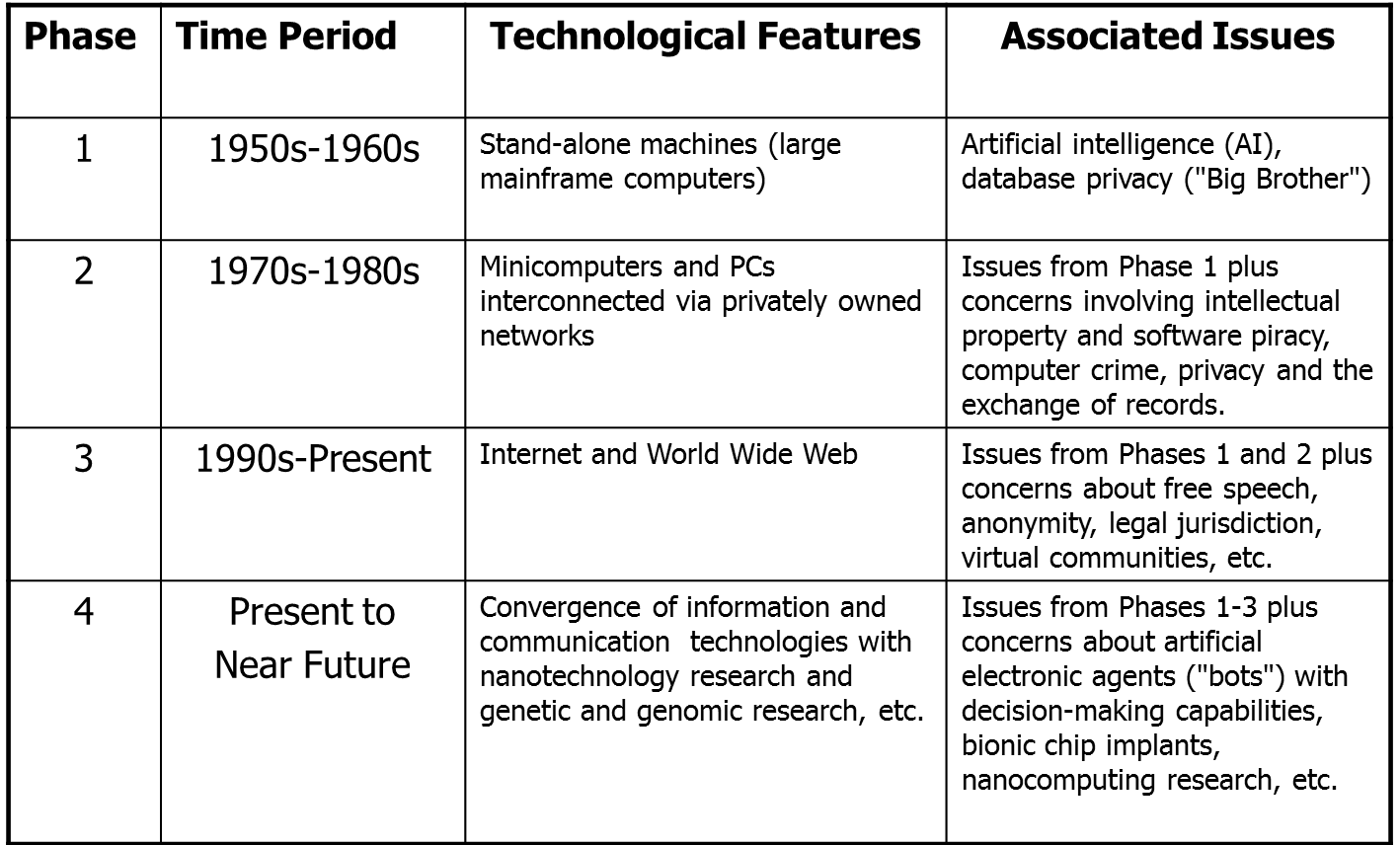
## Networked devices can be connected directly to the Internet. They also can be connected to other devices through one or more privately owned computer networks. Privately owned networks include both Local Area Networks (LANs) and Wide Area Networks (WANs).

* **Why the term cyberethics?**

## Cyberethics is a more accurate label than computer ethics, which might suggest the study of ethical issues limited to computing machines, or to computing professionals.

## It is more accurate than Internet ethics, which is limited only to ethical issues affecting computer networks.

## **Table 1-1: Summary of Four Phases of Cyberethics**



**5.2 Are Cyberethics Issues Unique?**

## Consider the Amy Boyer case of cyberstalking in light of issues raised. Is there anything new or unique about this case from an ethical point of view? Boyer was stalked in ways that were not possible before cybertechnology. But do new ethical issues arise?

## Two points of view:

## Traditionalists argue that nothing is new – crime is crime, and murder is murder.

## Uniqueness Proponents argue that cybertechnology has introduced (at least some) new and unique ethical issues that could not have existed before computers.

## Both sides seem correct on some claims, and both seem to be wrong on others. Traditionalists underestimate the role that issues of scale and scope that apply because of the impact of computer technology.

## Cyberstalkers can stalk multiple victims simultaneously (scale) and globally (because of the scope or reach of the Internet).

## They also can operate without ever having to leave the comfort of their homes. Uniqueness proponents tend to overstate the effect that cybertechnology has on ethics per se. Maner (1996) argues that computers are uniquely fast, uniquely malleable, etc. There may indeed be some unique aspects of computer technology. But uniqueness proponents tend to confuse unique features of technology with unique ethical issues. They use the following logical fallacy:

## Cybertechnology has some unique technological features.

## Cybertechnology generates ethical issues.

## Therefore, the ethical issues generated by cybertechnology must be unique.

## Traditionalists and uniqueness proponents are each partly correct. Traditionalists correctly point out that no new ethical issues have been introduced by computers. Uniqueness proponents are correct in that cybertechnology has complicated our analysis of traditional ethical issues.

## So we must distinguish between:

## (a) Unique technological features

## (b) Any (alleged) unique ethical issues

## Two scenarios from the text:

## (a) Computer professionals designing and coding a controversial computer system

## (b) Software piracy

**5.3Case Illustration of a Policy Vacuum: Duplicating Software**

## In the early 1980s, there were no clear laws regarding the duplication of software programs, which was made easy because of personal computers. A policy vacuum arose. Before the policy vacuum could be filled, we had to clear up a conceptual muddle: What exactly is software?

* **Cyberethics as a Branch of Applied Ethics**

## Applied ethics, unlike theoretical ethics, examines "practical" ethical issues. It analyzes moral issues from the vantage-point of one or more ethical theories. Ethicists working in fields of applied ethics are more interested in applying ethical theories to the analysis of specific moral problems than in debating the ethical theories themselves.

## Three distinct perspectives of applied ethics (as applied to cyberethics):

## Professional Ethics

## Philosophical Ethics

## Descriptive Ethics

* **Perspective # 1: Professional Ethics**

## According to this view, cyberethics is the field that identifies and analyzes issues of ethical responsibility for computer professionals. Consider a computer professional's role in designing, developing, and maintaining computer hardware and software systems.

## Suppose a programmer discovers that a software product she has been working on is about to be released for sale to the public, even though it is unreliable because it contains "buggy" software.

## Should she "blow the whistle?"

## Don Gotterbarn (1991) argued that all genuine computer ethics issues are professional ethics issues. Computer ethics, for Gotterbarn is like medical ethics and legal ethics, which are tied to issues involving specific professions. He notes that computer ethics issues aren’t about technology – e.g., we don’t have automobile ethics, airplane ethics, etc.

* **Criticism of Professional Ethics Perspective**

## Gotterbarn’s model for computer ethics seems too narrow for cyberethics. Cyberethics issues affect not only computer professionals; they affect everyone. Before the widespread use of the Internet, Gotterbarn’s professional-ethics model may have been adequate.

* **Perspective # 2: Philosophical Ethics**

## From this perspective, cyberethics is a field of philosophical analysis and inquiry that goes beyond professional ethics (Gotterbarn). Moor (1985), defines computer ethics as *“the analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology”.*

## Moor argues that automobile and airplane technologies did not affect our social policies and norms in the same kinds of fundamental ways that computer technology has.

## Automobile and airplane technologies have revolutionized transportation, Resulting in our ability to travel faster and farther than was possible in previous eras, but they did not have the same impact on our legal and moral systems as cybertechnology.

* **Philosophical Ethics: Standard Model of Applied Ethics**

## Philip Brey (2000) describes the “standard methodology” used by philosophers in applied ethics research as having three stages:

## 1) Identify a particular controversial practice as a moral problem.

## 2) Describe and analyze the problem by clarifying concepts and examining the factual data associated with that problem.

## 3) Apply moral theories and principles to reach a position about the particular moral issue.

* **Perspective #3: Cyberethics as a Field of Descriptive Ethics**

## The professional and philosophical perspectives both illustrate normative inquiries into applied ethics issues. Normative inquiries or studies are contrasted with descriptive studies.

## Descriptive investigations report about "what is the case“; normative inquiries evaluate situations from the vantage-point of the question: "what ought to be the case."

## Scenario: A community’s workforce and the introduction of a new technology. Suppose a new technology displaces 8,000 workers in a community. If we analyze the issues solely in terms of the number of jobs that were gained or lost in that community, our investigation is essentially descriptive in nature. We are simply describing an impact that technology X has for Community Y.

## Descriptive vs. Normative Claims

## Consider three assertions:

## (1) "Bill Gates served as the Chief Executive Officer of Microsoft Corporation for many years.”

## (2) "Bill Gates should expand Microsoft’s product offerings”

## (3) “Bill Gates should not engage in business practices that are unfair to competitors.”

## Claims (2) and (3) are normative, (1) is descriptive; (2) is normative but nonmoral, while (3) is both normative and moral.

# 

## **Figure 1-1: Descriptive vs. Normative Claims**

* **Some Benefits of Using the Descriptive Approach**

## Huff & Finholt (1994) claim that when we understand the descriptive aspect of social effects of technology, the normative ethical issues become clearer.

## The descriptive perspectives prepare us for our subsequent analysis of ethical issues that affect our system of policies and laws.

## **Table 1-2: Summary of Cyberethics Perspectives**

**5.4 Is Cyber-technology Neutral?**

## Technology seems neutral, at least initially. Consider the cliché: “Guns don’t kill people, people kill people.” Corlann Gee Bush (19997) argues that gun technology, like all technologies, is biased in certain directions. She points out that certain feature inherent in gun technology itself cause guns to be biased in a direction towards violence.

## Bush uses an analogy from physics to illustrate the bias inherent in technology. An atom that either loses or gains electrons through the ionization process becomes charged or valenced in a certain direction. Bush notes that all technologies, including guns, are similarly valenced in that they tend to "favor" certain directions rather than others.

## Thus technology is biased and is not neutral.

* **A "Disclosive" Method for Cyberethics**

## Brey (2001) believes that because of embedded biases in cybertechnology, the standard applied-ethics methodology is not adequate for identifying cyberethics issues.

## We might fail to notice certain features embedded in the design of cybertechnology. Using the standard model, we might also fail to recognize that certain practices involving cybertechnology can have moral implications.

## Brey notes that one weakness of the “standard method of applied ethics” is that it tends to focus on known moral controversies. So that model fails to identify those practices involving cybertechnology which have moral implications but that are not yet known.

## Brey refers to these practices as having morally opaque (or morally non-transparent) features, which he contrasts with "morally transparent” features.

## 

## **Figure 1-2: Embedded Technological Features Having Moral Implications**

* **A Multi-Disciplinary & Multi-Level Method for Cyberethics**

## Brey’s “disclosive method” is multidisciplinary because it requires the collaboration of computer scientists, philosophers, and social scientists.

## It also is multi-level because the method for conducting computer ethics research requires the following three levels of analysis:

### Disclosure level

### Theoretical level

### Application level

# **Table 1-3: Three Levels in Brey’s “Disclosive Model”**

# 

* **Three-step Strategy for Approaching Cyberethics Issues**

## **Step 1.** Identify a practice involving cyber-technology, or a feature in that technology, that is controversial from a moral perspective.

## 1a. Disclose any hidden (or opaque) features or issues that have moral implications

## 1b. If the issue is descriptive, assess the sociological implications for relevant social institutions and socio-demographic and populations

## 1c. If there are no ethical/normative issues, then stop.

## 1d. If the ethical issue is professional in nature, assess it in terms of existing codes of conduct/ethics for relevant professional associations (see Chapter 4).

## 1e. If one or more ethical issues remain, then go to Step 2.

## **Step 2**. Analyze the ethical issue by clarifying concepts and situating it in a context.

## 2a. If a policy vacuums exists, go to Step 2b; otherwise go to Step 3.

## 2b. Clear up any conceptual muddles involving the policy vacuum and go to Step 3.

## **Step 3.** Deliberate on the ethical issue. The deliberation process requires two stages:

## 3a. Apply one or more ethical theories (see Chapter 2) to the analysis of the moral issue, and then go to step 3b.

## 3b. Justify the position you reached by evaluating it against the rules for logic/critical thinking

Lecture 07

Ethical and Social Issues in Information Systems

**7.1 Introduction**

While studying Ethical and Social Issues in Information Systems, the following questions need to be answered:

## What ethical, social, and political issues are raised by information systems?

## What specific principles for conduct can be used to guide ethical decisions?

## Why do contemporary information systems technology and the Internet pose challenges to the protection of individual privacy and intellectual property?

## How have information systems affected everyday life?

* **Behavioral Targeting and Your Privacy: You’re the Target**

Problem: Need to efficiently target online ads

Solutions: Behavioral targeting allows businesses and organizations to more precisely target desired demographics. Google monitors user activity on thousands of sites; businesses monitor own sites to understand customers. Demonstrate its role in organizing and distributing information. Illustrates the ethical questions inherent in online information gathering

**7.2 Understanding Ethical and Social Issues Related to Systems**

**Recent cases of failed ethical judgment in business:**

## Lehman Brothers, Minerals Management Service, Pfizer

## In many, information systems used to bury decisions from public scrutiny

**Ethics:**

## Principles of right and wrong that individuals, acting as free moral agents, use to make choices to guide their behaviors

**Information systems and ethics:** Information systems raise new ethical questions because they create opportunities for:

## Intense social change, threatening existing distributions of power, money, rights, and obligations

## New kinds of crime

## **Model for thinking about ethical, social, political issues:**

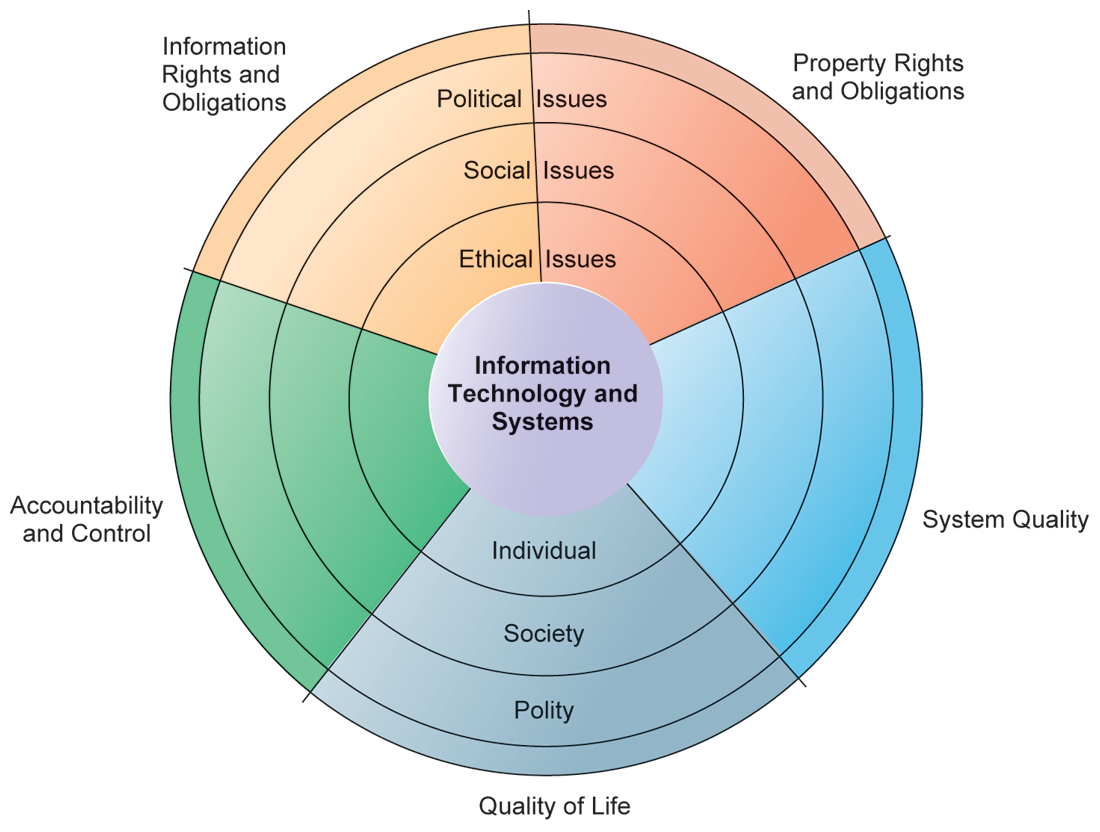
## Society as a calm pond

## IT as rock dropped in pond, creating ripples of new situations not covered by old rules

## Social and political institutions cannot respond overnight to these ripples—it may take years to develop etiquette, expectations, laws

## Requires understanding of ethics to make choices in legally gray areas

* **The Relationship Between Ethical, Social, and Political Issues in An Information Society**



**Figure 4-1: The Relationship between Ethical, Social, and Political Issues in an Information Society**

## The introduction of new information technology has a ripple effect, raising new ethical, social, and political issues that must be dealt with on the individual, social, and political levels. These issues have five moral dimensions: information rights and obligations, property rights and obligations, system quality, quality of life, and accountability and control.

## **Five moral dimensions of the information age**

## Information rights and obligations

## Property rights and obligations

## Accountability and control

## System quality

## Quality of life

**7.3 Key technology trends that raise ethical issues**

### **Doubling of computer power**

## More organizations depend on computer systems for critical operations

### **Rapidly declining data storage costs**

## Organizations can easily maintain detailed databases on individuals

### **Networking advances and the Internet**

## Copying data from one location to another and accessing personal data from remote locations is much easier

### **Advances in data analysis techniques**

## Companies can analyze vast quantities of data gathered on individuals for:

### **Profiling**

## Combining data from multiple sources to create dossiers of detailed information on individuals

### **Nonobvious relationship awareness (NORA)**

## Combining data from multiple sources to find obscure hidden connections that might help identify criminals or terrorists

Lecture 08

Ethical and Social Issues in Information Systems (Continued)

**8.1 Nonobvious Relationship Awareness (Nora)**

## NORA technology can take information about people from disparate sources and find obscure, nonobvious relationships. It might discover, for example, that an applicant for a job at a casino shares a telephone number with a known criminal and issue an alert to the hiring manager.

## **Fig-4-01.png**

**Figure 4-2: Nonobvious Relationship Awareness (Nora)**

* **Ethics in an Information Society**

## **Basic concepts for ethical analysis**

### **Responsibility:** Accepting the potential costs, duties, and obligations for decisions

### **Accountability:** Mechanisms for identifying responsible parties

### **Liability:** Permits individuals (and firms) to recover damages done to them

### **Due process:** Laws are well known and understood, with an ability to appeal to higher authorities

## **Ethical analysis: A five-step process**

## Identify and clearly describe the facts

## Define the conflict or dilemma and identify the higher-order values involved

## Identify the stakeholders

## Identify the options that you can reasonably take

## Identify the potential consequences of your options

## **Six Candidate Ethical Principles**

## **Golden Rule**

## Do unto others as you would have them do unto you

## **Immanuel Kant’s Categorical Imperative**

## If an action is not right for everyone to take, it is not right for anyone

## **Descartes’ Rule of Change**

## If an action cannot be taken repeatedly, it is not right to take at all

## **Utilitarian Principle**

## Take the action that achieves the higher or greater value

## **Risk Aversion Principle**

## Take the action that produces the least harm or least potential cost

## **Ethical “no free lunch” Rule**

## Assume that virtually all tangible and intangible objects are owned by someone unless there is a specific declaration otherwise

## **Professional codes of conduct**

## Promulgated by associations of professionals

## E.g. AMA, ABA, AITP, ACM

## Promises by professions to regulate themselves in the general interest of society

## **Real-world ethical dilemmas**

## One set of interests pitted against another

## E.g. Right of company to maximize productivity of workers vs. workers right to use Internet for short personal tasks

**8.2 The Moral Dimensions of Information Systems**

## **Privacy:**

## Claim of individuals to be left alone, free from surveillance or interference from other individuals, organizations, or state. Claim to be able to control information about yourself

## **In U.S., privacy protected by:**

## First Amendment (freedom of speech)

## Fourth Amendment (unreasonable search and seizure)

## Additional federal statues (e.g. Privacy Act of 1974)

## **Fair information practices:**

## Set of principles governing the collection and use of information. It is basis for most U.S. and European privacy laws. These are based on mutuality of interest between record holder and individual. Restated and extended by FTC in 1998 to provide guidelines for protecting online privacy. Used to drive changes in privacy legislation

## COPPA

## Gramm-Leach-Bliley Act

## HIPAA

## **FTC FIP principles:**

## Notice/awareness (core principle)

## Choice/consent (core principle)

## Access/participation

## Security

## Enforcement

Lecture 09

Ethical and Social Issues in Information Systems (continued)

**9.1 Learning Objectives**

## What ethical, social, and political issues are raised by information systems? What specific principles for conduct can be used to guide ethical decisions? Why do contemporary information systems technology and the Internet pose challenges to the protection of individual privacy and intellectual property? How have information systems affected everyday life?

**The Moral Dimensions of Information Systems**

* **European Directive on Data Protection:**

## Requires companies to inform people when they collect information about them and disclose how it will be stored and used. Requires informed consent of the customers, EU member nations cannot transfer personal data to countries with no similar privacy protection (e.g. U.S.)

## U.S. businesses use safe harbor framework, self-regulating policy to meet objectives of government legislation without involving government regulation or enforcement.

* **Internet Challenges to Privacy:**

## **Cookies**

## Tiny files downloaded by Web site to visitor’s hard drive to help identify visitor’s browser and track visits to site

## Allow Web sites to develop profiles on visitors

## **Web beacons/bugs**

## Tiny graphics embedded in e-mail and Web pages to monitor who is reading message

## **Spyware**

## Surreptitiously installed on user’s computer

## May transmit user’s keystrokes or display unwanted ads

## **Google’s collection of private data; behavioral targeting**

* **How Cookies Identify Web Visitors**

## Cookies are written by a Web site on a visitor’s hard drive. When the visitor returns to that Web site, the Web server requests the ID number from the cookie and uses it to access the data stored by that server on that visitor. The Web site can then use these data to display personalized information.

## **Fig-4-03.png**

## **Figure 4-3: How Cookies Identify Web Visitors**

## U.S. allows businesses to gather transaction information and use this for other marketing purposes

## Online industry promotes self-regulation over privacy legislation. However, extent of responsibility taken varies

## Statements of information use

## Opt-out selection boxes

## Online “seals” of privacy principles

## Most Web sites do not have any privacy policies

* **Technical solutions**

## **The Platform for Privacy Preferences (P3P)**

## Allows Web sites to communicate privacy policies to visitor’s Web browser – user. User specifies privacy levels desired in browser settings. E.g. “medium” level accepts cookies from first-party host sites that have opt-in or opt-out policies but rejects third-party cookies that use personally identifiable information without an opt-in policy.

* **The P3P Standard**

## P3P enables Web sites to translate their privacy policies into a standard format that can be read by the user’s Web browser software. The browser software evaluates the Web site’s privacy policy to determine whether it is compatible with the user’s privacy preferences.

## **Fig-4-03.png**

## **Figure 4-4: The P3P Standard**

* **Property rights: Intellectual property**

### Intellectual property: Intangible property of any kind created by individuals or corporations. Three main ways that protect intellectual property

### Trade secret: Intellectual work or product belonging to business, not in the public domain

### Copyright: Statutory grant protecting intellectual property from being copied for the life of the author, plus 70 years

### Patents: Grants creator of invention an exclusive monopoly on ideas behind invention for 20 years

## **Challenges to intellectual property rights**

### Digital media different from physical media (e.g. books)

## Ease of replication

## Ease of transmission (networks, Internet)

## Difficulty in classifying software

## Compactness

## Difficulties in establishing uniqueness

## **Digital Millennium Copyright Act (DMCA)**

### Makes it illegal to circumvent technology-based protections of copyrighted materials

## **Accountability, Liability, Control**

### Computer-related liability problems, if software fails, who is responsible?

### If seen as part of machine that injures or harms, software producer and operator may be liable. If seen as similar to book, difficult to hold author/publisher responsible. What should liability be if software seen as service? Would this be similar to telephone systems not being liable for transmitted messages?

## **System Quality: Data Quality and System Errors**

### What is an acceptable, technologically feasible level of system quality?

## Flawless software is economically unfeasible

### Three principal sources of poor system performance:

## Software bugs, errors

## Hardware or facility failures

## Poor input data quality (most common source of business system failure)

## **Quality of life: Equity, access, and boundaries**

### Negative social consequences of systems

### Balancing power: Although computing power decentralizing, key decision-making remains centralized.

### Rapidity of change: Businesses may not have enough time to respond to global competition

### Maintaining boundaries: Computing, Internet use lengthens work-day, infringes on family, personal time.

### Dependence and vulnerability: Public and private organizations ever more dependent on computer systems.

## **Computer crime and abuse**

### Computer crime: Commission of illegal acts through use of compute or against a computer system, computer may be object or instrument of crime.

### Computer abuse: Unethical acts, not illegal

### Spam: High costs for businesses in dealing with spam

## **Employment:** Reengineering work resulting in lost jobs

## **Equity and access – the digital divide:** Certain ethnic and income groups in the United States less likely to have computers or Internet access.

Lecture 10

Social Media and its Impacts on Society

**10.1 What Is Social Media?**

Social media is the use of web-based technologies allowing the creation and exchange of user-generated content. Blending of technology and social, the “social” in social media implies a conversation. The difference between social media and the TV is that with the latter, viewers seldom engage with the programme-makers of the show that they are watching. Only in very recent times have programme makers expanded into the world of social media. Think X-Factor.



**Figure 10.1: Famous Social Medias**

## The Central Office of Information (www.coi.gov.uk) said the following in its 2009 publication “Engaging through Social Media”: “*Social media is a term used to refer to online technologies and practices that are used to share opinions and information, promote discussion and build relationships. Social media services and tools involve a combination of technology, telecommunications and some kind of social interaction. They can use a variety of different formats, for example text, pictures, video and audio”.*

## Social media is different to traditional forms of communication such as through newspapers, television, and film.

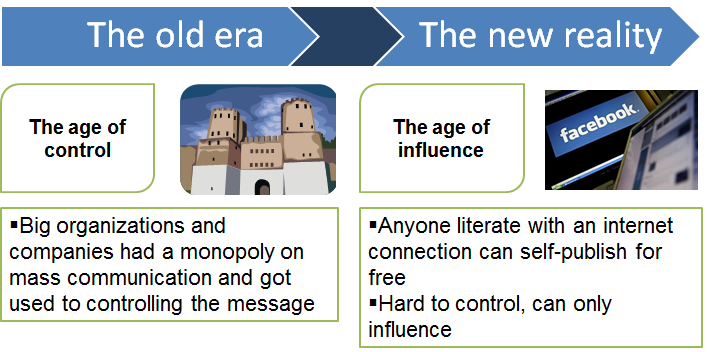
## **Cheap** – anyone with access to the internet (for example through public libraries)

## **Accessible** – the tools are easy to use

## **Enabling** – allows almost anyone to do things that previously were only the preserve of well-resourced organisations

## The use of the word “Social” implies a conversation. Social media is definitely not about one-way communication to a large audience from big organisations.

**Megatrends 1 – The death of control**

****

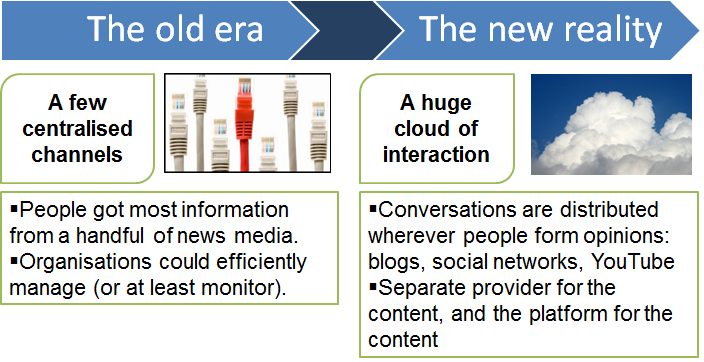
**Figure 10.2: The death of control**

**Megatrends 2 – Fewer gatekeepers**

# 

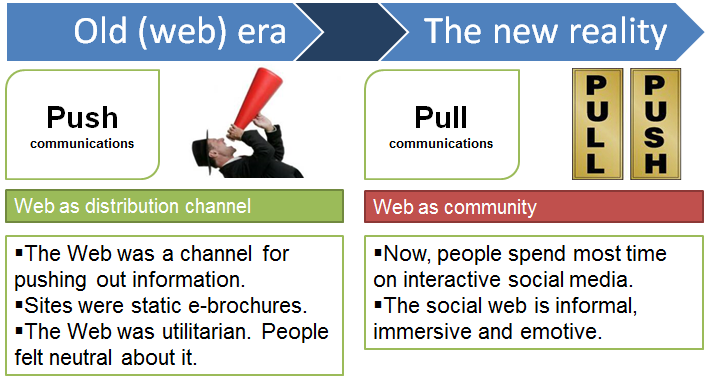
**Figure 10.3: Fewer gatekeepers**

**Megatrends 3 – Fragmentation**

****

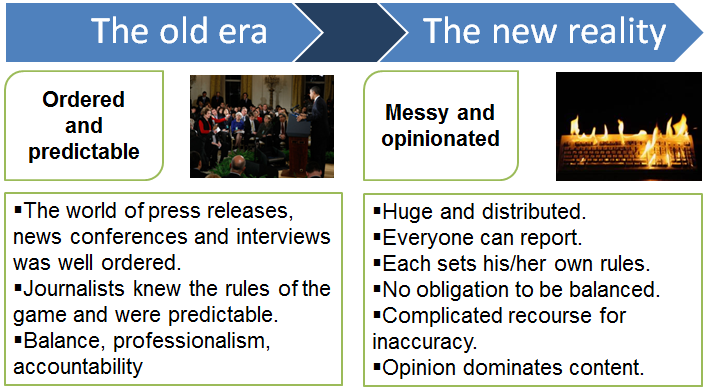
**Figure 10.4: Fragmentation**

**Megatrends 4 – New web landscape**

****

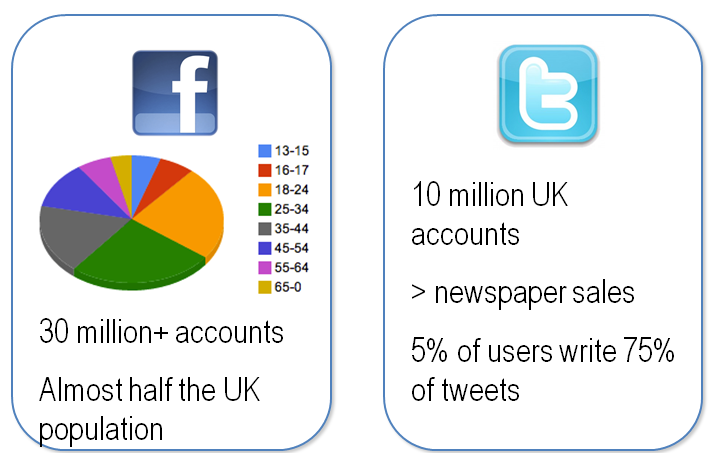
**Figure 10.5: New web landscape**

**Megatrends 5 – New journalism**

****

**Figure 10.6: New journalism**

**How big is social media in the UK?**

****

**Figure 10.7: Social Media (UK)**

**10.2 Social Media Impact**

## Social networks are moving towards payments on those platforms (eg, Facebook or using Bit coins). Payments (especially mobile) are making connections with social networks similar to how PayPal revolutionized industry. Social Media can quickly and positively or adversely affect company reputation.

## Linked In: ww.linkedin.com: 100mm users worldwide, 44mm US

## Facebook: www.facebook.com: 175mm users worldwide

## Twitter: www.twitter.com: 200mm users worldwide

**That’s great for the industry, but why am I utilizing Social Media?**

## Industry knowledge: Almost impossible to keep up with all industry publications, becoming connected helps pinpoint hot issues. Building a personal brand: Keep your contacts and maintain knowledge even when changing companies or careers, develops a more comprehensive skill set.

## Becoming more effective at networking: A large network helps you connect to people even when you can’t help them personally, networks should expand beyond core business contacts and companies

Lecture 11

Social Media and its Impacts on Society (Continues)

**11.1 Social Media Circles**

## Payments industry uses

## LinkedIn

## Blogs/Discussion forums

## YouTube

## Lesser Extent: Twitter and Facebook

## However, Facebook has just launched Branch Out

##### Professional networking using FB’s reach

* **LinkedIn**

## Build your network:

##### Stay in touch with current and former peers

##### Create community, expand contact lists and introduce connections

## Showcasing skill set:

##### Publishing your resume or establishing expertise for potential clients or employers to view

## Work your network, make yourself visible:

##### Join groups, gather relevant information, participate in discussions, receive industry updates as they occur

## Find targeted people with a specific skill sets

##### For hiring or informational/networking purposes

## JOB SEARCH: Utilized to find jobs, people and business opportunities recommended by someone in one's contact network – levels 1,2,3

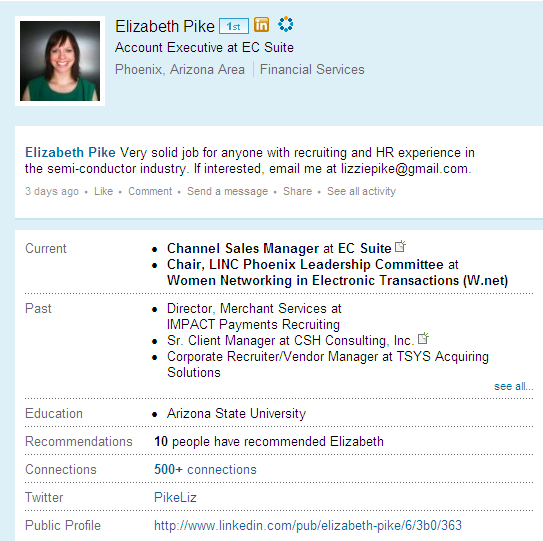
## TALENT SEARCH: Employers can list jobs and search for potential candidates

## NETWORKING RESOUCE: Members can review circle profiles of to determine which of their existing contacts can introduce them to people they want to know

## PERSONAL-PROFESSIONAL BRANDING: Users can post their own photos and view photos of others to aid in identification

## INDUSTRY UPDATE RESOURCE: Register to follow companies to get notifications and relevant information

## INFORMATION PORTAL: Users can bookmark (profiles, jobs, etc.) to return to for future reference



**Figure 10.8: A Sample Linkedin Profile View**

# **Maximizing LinkedIn**

## Strive for 100% completeness on profile and keep updated (new skill sets, new company). Continue to reach out, make connections, or reply to conversations –this pops up on your connection’s activity feed. Post events or new products/information. Follow companies, join and create group. Helpful for industry info, adding contacts to network and all groups have a job posting capability

# PPTAC.png

**Figure 10.9: A Sample Linkedin Recommendations View**

# **Marketing your Profile**

## Include a LinkedIn link on your signature

## Ask for recommendations after completing business

## Integrate business tweets

## Optimize your profile

## Focus on developing a quality network

# **Blogs and Discussion Forums**

## Receive real time industry updates

## Search for new product releases

## Expand marketing tools for customer base

## Reach new clients

## Follow and engage in industry discussions

## Serves as a ‘classifieds’ page or open source link

## **You Tube**

## Showcase products:

## Compare speed between dial up and wireless terminals

## Launch new marketing campaigns for companies, act as a commercial for company

## Demos for new products/services

## Build personal-professional brand

# **Twitter**

## Micro blogging site

## Sharing of industry information/updates, usually through sharing links

## Can be useful in following new companies and their technology

## Receive up to date info through following active users

## Conversation starter

## Forum to create company buzz

## External campaigns or contests

# **Facebook**

## Becoming an important marketing strategy to increase brand awareness and customer loyalty

## i.e. “LIKE” button

## Facebook has wider reach but more casual than LinkedIn

## Mixed audiences can become tricky

## Introducing Branch Out

## http://branchout.com/about/productTour

Lecture 12

Social Media and its Impacts on Society (Continues)

**12.1 Social Media: Differentiating Your Unique Brand**

## If you are in a mid-size or larger company, your company probably has an integrated marketing social media business plan, but YOU are also your own brand. How can you most effectively utilize social media in your life?

# **Enhance Social Media with Cross Links**

## Helps contacts, customers and potential clients find you and keep you as a source for information

## Tells search engines (like Google or Bing) that your social profiles are all related: Pre-emptively occupies Google Page 1, making it more difficult for negative press to float to top.

## Syndicates content: Reduces the need to create new content for every site daily

# **Tips to Enhance Social Media Platforms**

## If utilizing Facebook for professional reasons, best to create two accounts –one linked with professional, and one personal and private

## Can cross link: e.g. social media icons on website, blogs that link to LI, Facebook, Twitter, LinkedIn can integrate Twitter feed

## Participate in conversations about your industry, can set up reminders via free tools to flag keywords (industry, competitor names) –Hootsuite, GoogleAlerts, TweetDeck, Socialmention.com

# **Integrating Social Media**

## Choose the platforms that will enhance your business initiative

### You don’t need to join every site, and it’s useless to join if you aren’t interacting.

### Understand the site’s culture and/or rules

### Sometimes unspoken

## Stay relevant and top of mind

### Follow through on commitments

### Thank others for helping you

### Do what you say you will, and thank others for helping you

# **Types of social networkers**

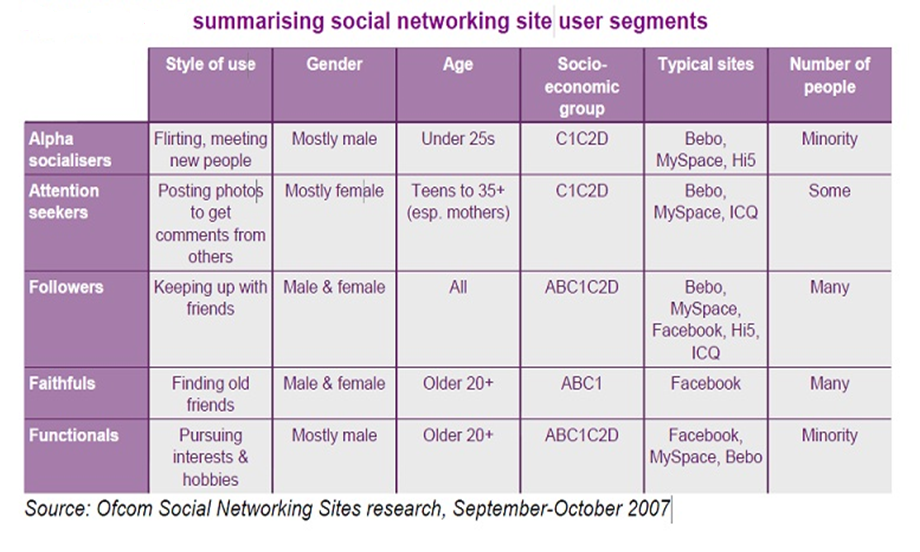
## Alpha Socialisers – (a minority) people who used sites in intense short bursts to flirt,meet new people, and be entertained.

## Attention Seekers – (some) people who craved attention and comments from others,often by posting photos and customising their profiles.

## Followers – (many) people who joined sites to keep up with what their peers were doing.

## Faithfuls – (many) people who typically used social networking sites to rekindle old friendships, often from school or university.

## Functionals – (a minority) people who tended to be single-minded in using sites for a particular purpose.



**Figure 10.10: Social Networking Sites/User Segments**

# **Privacy concerns**

## Social networking sites provide privacy options but users are generally unaware or tend to ignore such concerns. Stalkers, terrorists, ill-doers, con-artists could benefit from such issues. Recent scandals-England: MI-6’s director’s wife puts up photos of family on facebook. Facebook’s controversial decision to make visible relationship actions to entire social group

# **Security issues**

## Recent malware exploiting social networks

### Malicious Banner ads

### Adware

### Phishing attacks

### Customizable scripts

Lecture 13  
Ethics and Social Media

**13.1 Why Ethics?**

Technology advances faster than ethical values, morals and especially laws Discussion between relevant parties needed, ethicists, professionals, ’intelligentsia’, organisation representatives, politicians, media, ’normal’ people, etc. Law and morals do not always meet.

* **Motivation**

**Vacuum of rules**

Rules of the field derived from old rules, there aren’t any rules or they aren’t followed

**Conceptual muddles**

Is a program a service, means of production, idea or a presentation of an idea?

**Social use environment**

ICT artefacts are seldom private affairs anymore

* **New questions?**

New area: Old questions or new area with new questions? Does the medium bring new ethical questions to bear? Is there something fundamentally different about ICT compared to other things?

**Ethics, Applied Ethics and Morals**

Ethics is the study of morals. Morals are the (right or good) habits which people have in a society (lat. mores). Applied ethics tries to clarify the questions of ethics/morals so that they can be discussed, professional ethics within a field. Ethics have been and are still used to formulate policies in societies.

**The aim(s) of Ethics**

**The good of the people**

* To understand what it would be – Meta ethics
* To build a system(s) to solve how to get there
* To apply the system(s) to actual questions coherently and consistently
* To aid us in our moral problems and to give descriptions of what ethical positions people hold
* **Some ethical theories (and their applications)**

Virtue ethics (Aristoteles, MacIntyre, others): Moral character of a person 🡪 professional ethics?

Ethics of friendship – online?: Telos (an ultimate aim or object), the meaning of life

Utilitarianism or Consequentialism (Mill, Bentham): The greatest amount of good for (the greatest amount of) people

**Deontology, duty ethics (Kant, Rawls)**

* We have duties to others
* Never treat another person *merely* as means, but always as an end in themselves
* Universal moral law
* Voluntary action

**Rights based theories (Locke, Rawls)**

* Classic Liberalism, Libertarianism
* Communitarianism, Socialism, Social Democracy

**13.2 Social Media: Examples of Issues**

* Privacy
* Property
* Teaching
* Friendship

Lecture 14  
Ethics and Social Media

**14.1 Privacy questions different to ’traditional’ issues**

”Forgive and forget” does not exist anymore. What was once on-line, can be found always (Blanchette & Johnson, 2002)

* Obligation to protect the future privacy interests of children/teens? (Bülow & Wester, 2011)
* Streisand effect (residence of the singer)

Concept of privacy changing

* Everyone makes mistakes
* No one is expected to be ’perfect’

Since what one has done is always available, one is expected to always be same?

**Expectations of on-line privacy**

Can we expect to not be known?

Writing to IRC, other chat, bulletin board or blog / newspaper comments section, expecting to be ‘anonymous’

* Is a ‘nick’ with no identifying information some sort of guarantee for anonymity?
* A lot of information available in many cases
* Searches to identify etc

Internet ‘discussions’ not similar to physical discussions, anyone can log them and find the information later

* People generally think that they have more privacy than they actually do
* On-line monitoring, “spyware”—one generally does not know when one is logged/monitored

In (open) Blogs there can be no expectation of privacy – even if written with a ‘nick’ (Grodzinsky & Tavani, 2009)

**Privacy in SoMes**

Public and private blur – in SoMes it is difficult to control the audiences of ones posts (see e.g. Netchitailova, 2011 on Facebook).

Most people just do not bother, but the added illusion of anonymity promotes writing things one would not divulge of one’s private life, say, in Blogs or similar.

Also, some groups (such as children and/or elderly – for different reasons) have undue trust to hand over their private information to outsiders (See e.g. Chai et al., 2008).

Pictures in SoMes?

* Does anyone ever ask whether the pictures they take can be published? Most often not. (Parrish, 2010, Cammozzo, 2011.)
* Typically, this not a problem, but what about, say the Arab Spring? How many have actually been killed due to having been identified from pictures? (on Iranian elections of 2009 and the following riots, see Parrish, 2010. Also see Asai, 2011 on Tunisia and Egypt.)

**Children and young people**

**Children’s privacy**

* ‘Funny pictures’ parents put on a SoMe may come to light – we know how cruel children can be, and adults do not always think what they put on social media
* Vlogging (Ahmed, 2011a) as an example of potential privacy harm for children.
* Pictures/video breaching privacy can be uploaded easily enough – and distributed widely (see e.g. Khan, 2008 amongst others).

Many younger users of SoMes are willing to trade a lot of their privacy for the (perceived) gains offered by SoMes

* They seem to be quite aware of the loss of privacy – and concerned.
* However, the perceived benefits override their concern for privacy; especially in the case of ‘heavy users’. (Gumbus, Grodzinsky & Lilley, 2010.)

**Property (immaterial)**

**Law**

* We know what the law states – or do we?

**User Generated Content**

* Relation to commercial content

**What is legal and what is right do not always meet**

* Basically all younger generation members have mixed or used copyright protected materials illegally (or at least without permission)
* Are we all criminals online? (Hielkema et al., unpublished)

**Work**

Workplace policies were primarily focused on eMail and Internet usage while at work. Now SoMes need to be taken into account as well. Blurring of the line between work use and private use

* Lap-tops, corporate ’tax-phones’ (multi-media devices), etc

**For high-end specialists – *results* what matters**

* So ’waste-of-time’ argument irrelevant, unless clearly a problem

Security question though; what work related info can be distributed in SoMes and what not?

Corporate image vs. private/professional image

Professionals need Internet presence – otherwise they do not exist in today’s work market…

* Positive Internet presence – how to do this whilst avoiding ”Streisand effect”? Be careful on what narrative bits you post in SoMes
* ’Professional brand’

(Gotterbarn, 2011, Mitra, 2011)

Lecture 15  
Ethics and Social Media

**15.1 Marketing**

We give our data to services such as Facebook. Mining the data directs the marketing – and increases it. New ways (or ’old’ ways in new environment) of marketing in Facebook?.

Users oppose the practice, but use anyway?. Perceived benefits (see before)

(Lilley, Grodzinsky & Gumbus, 2011)

**Teaching**

**A course in 2nd life; can it be expected that:**

* Students will use a third party service?
* Teachers put their materials (at least in part) available in a resource they cannot control – the EULA of which they likely do not even know/understand?
* Use of service not controlled by the employer
* What if the service is no longer available – what happens to content created within?

What about developing countries?

Can Web 2.0 applications bring benefits?

Limited resources – but if access to Internet, materials/discussions etc. available through SoMes

* Wikis
* Blogs
* Other social networks

(Ahmed, 2011b)

**“The Other”**

SoMe users are (typically) other human beings

This tends to be forgotten, or at least distancing can (and often does) happen

* Hurt in SoMe = hurt IRL!

eIdentity – who/what am I in SoMe?

* Who/what am I IRL? Lecturer, researcher, colleague, father, friend, pal, acquaintance, etc.
* SoMes: Chat(s), Boards, Virtual Worlds, Games, Wikis, etc.
* (Perceived) anonymity (when wanted) – IRL?
* One can change more of oneself than one can in IRL
* A/S/L, etc. – be who you want to be, not who you happen to be!

**Friendship**

**What is friendship?**

* Aristoteles – telos/character

**Can real friendship be formed in SoMes?**

* Say, through Facebook or … Twitter?
* (IR)Chat?
* MMO(RPG)s?

**Is it always just a lame replacement of The Real Thing ™?**

Unless there is also an IRL connection

IRL friendship mediated through SoMe?

(See e.g. Briggle, 2009)

**Love in the SoMe era?**

**SoMes offer new kinds of possibilities for relationships**

* From ‘Platonic’ to sexual
* Easier to find similarly thinking people
* As an extreme example: Sexual racism in some dating services – black people only ’acceptable’ if conforming to stereotypes! (Coleman, 2011)
* Easier (?) to be deceived as well
* Easier to leave current relationship – knowledge that other kinds (‘the perfect’) exist!
* Can lead to less effort in existing relationship; and oth no replacement relationship…

(Ben-Ze'ev, 2011)

**“Third place/space”**

Home – family & friends

Work – colleagues, boss, etc.

SoMe? Claim (Asai, 2011) that this is ‘a third space’

Or, is it just an extension of the social/political space?

**The Political**

'age of fabricating the images‘ (Newman, 1999 – cited through the next reference)

“…fluid border between public (political) and personal sphere of human activity in the cyberspace”? (Churska-Nowak & Pawlak, 2011)

Blogs – see e.g. Halla-aho, Kasvi, or Soininvaara (with varying success)

FB/Twitter/… – see e.g. Obama (although also note the critique of this by Chomsky…)

**Terror in SoMes**

Due to Jihadists and other terrorrists having been driven out of Web 1.0 strategies, they have engaged in Facebook/Youtube

From top-to-bottom, one-to-many

To bottom-up, many-to-many

Professional media strategy

But harder to control.

(Gerdes, 2011)

**1 billion flies cannot be wrong**

**Generic theme in SoMes**

* Reddit main example: what is voted up is seen by users (Mills, 2011)
* But not only there, same happens in other SoMes as well – albeit, often dependant on the user choice
* Again, though, choosing, whose updates one sees

Even machines want to be our ’friends’ on Twitter (Mowbray, 2011)

**Literature**

* Feldman, Fred. (1978) Introductory Ethics, Prentice-Hall, Inc., Englewood Cliffs, N.J.
* Johnson, Deborah. Computer Ethics (eds. 2-4), 3rd ed. (2001) Prentice-Hall, Inc., Upper Saddle River, New Jersey.
* Pietarinen, Juhani & Seppo Poutanen. (1997) Etiikan teorioita, Turun yliopiston offsetpaino, Turku.
* Spinello, Richard (1995) Ethical Aspects of Information Technology Prentice-Hall.
* Weckert, John and Douglas Adeney (1997) Computers and Information Ethics, Greenwood Press.
* Tavani, Herman, T. (2007) Ethics & Technology, (2nd ed.), John Wiley & Sons, Inc., NJ, US.
* …and Platon, Aristoteles, Locke, Bentham, Mill, Kant, Rawls…
* Mike Leigh (2010) “Am I Bothered?” : Student Attitudes To Some Ethical Implications Of The Use Of Virtual Learning Environments Ethicomp 2010
* Ananda Mitra (2010) Multiple e-Identity Narratives in Social Networks
* Gotterbarn, Don and Moor, James (2009) Virtual Decisions: Just Consequentialism, Video game ethics, and Ethics on the fly, CEPE 2009, Corfu, Greece.
* Søraker, Johnny Hartz (2009) Virtually Good – What Can We Learn from the Argument from False Pleasures? CEPE 2009, Corfu, Greece.
* Briggle, Adam (2009) Computer-mediated Friendship: Illustrating Three Tasks for a Computer Ethics of the Good
* Nathaniel Adam Tobias Coleman (2011) “internet” = “intimate white intranet”: The ethics of online sexual racism Ethicomp 2011
* Malik Aleem Ahmed (2011a), Family Vlogging – Good or bad?, Ethicomp 2011
* Malik Aleem Ahmed (2011b) Social computing for expanding information capabilities of pre-service teachers in developing countries , Ethicomp 2011
* Alberto Cammozzo (2011) FACE RECOGNITION: PRIVACY ISSUES AND ENHANCING TECHNIQUES Ethicomp 2011
* Frances S. Grodzinsky, Herman T. Tavani (2008) Online File Sharing: Resolving the tensions between Privacy and Property Interests Ethicomp 2008
* Ekaterina Netchitailova (2011) Facebook: blurring of public and private. Ethicomp 2011
* Jean-François Blanchette & Deborah G. Johnson (2002) Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness, The Information Society Volume 18, Issue 1, 2002, 33—45
* Ghulam Ali Khan (2008) Security and Privacy in the Teaching of Islam and Globalization Ethicomp 2008
* Sangmi Chai, H. R. Rao, S. Bagchi-Sen, S. Upadhyaya (2008)'Wired' Senior Citizens and Online Information Privacy Ethicomp 2008
* Stephen Lilley, Andra Gumbus, Frances S. Grodzinsky (2010) What Matters To Non-Experts About Property And Privacy Rights? Ethicomp 2010
* Ryoko Asai (2011) Social Media as a Tool for Change Ethicomp 2011
* Aaron Ben-Ze'ev (2011) The Cyberspace Era: The Best and Worst of Times for Lovers Ethicomp 2011
* William Bülow, Misse Wester (2011) Autonomy and Privacy in the context of social networking Ethicomp 2011
* Karolina Churska-Nowak, Piotr Pawlak (2011) 'Growing role of the Internet services in political marketing. Social networks in use in political life'. Ethicomp 2011
* Anne Gerdes (2011) Online Radicalisation on YouTube and Facebook Ethicomp 2011
* Don Gotterbarn (2011) Tweeting is a beautiful sound, but not in my backyard: Employer Rights and the ethical issues of a tweet free environment for business. Ethicomp 2011
* Stephen Lilley, Frances S. Grodzinsky, Andra Gumbus, (2011) Facebook: Providing a Service to Members or a Platform to Advertisers? Ethicomp 2011
* Richard Mills (2011) Researching Social News – A novel forum for public discourse and information sharing. Ethicomp 2011
* Miranda Mowbray (2011) A Rice Cooker Wants to be my Friend on Twitter Ethicomp 2011

**Special Issue: Social Networking Sites, Number 2, June 2010 (and some from 3) of Ethics and Information Technology:**

* Michael Zimmer, ‘‘but the data is already public’’: on the ethics of research in Facebook
* Yoni Van Den Eede, ‘‘Conversation of Mankind’’ or ‘‘idle talk’’?: a pragmatist approach to Social Networking Sites
* David Wright & Kush Wadhwa, Mainstreaming the e-excluded in Europe: strategies, good practices and some ethical issues
* James L. Parrish Jr., PAPA knows best: Principles for the ethical sharing of information on social networking sites
* Shannon Vallor, Social networking technology and the virtues
* Christian Fuchs, studiVZ: social networking in the surveillance society
* Stephanie Patridge, The incorrigible social meaning of video game imagery
* Marcus Schulzke, Defending the morality of violent video games

**Special Issue: Friendship Online, Ethics and Information Technology: Volume 14, Number 3 / September 2012**

* Dean Cocking, Jeroen van den Hoven and Job Timmermans, Introduction: one thousand friends
* Shannon Vallor, Flourishing on facebook: virtue friendship & new social media
* Barbro Fröding and Martin Peterson, Why virtual friendship is no genuine friendship
* Johnny Hartz Søraker, How shall i compare thee? Comparing the prudential value of actual virtual friendship
* Michael T. McFall, Real character-friends: Aristotelian friendship, living together, and technology
* Robert Sharp, The obstacles against reaching the highest level of Aristotelian friendship online

Lecture 16  
Secure Social Networking

**16. 1 Overview**

## What is Social Networking?

## The Good, the Bad and the Ugly

## How to protect yourself

## How to protect your children

* **What is Social Networking?**

## **Wikipedia**

## A social network service focuses on building online communities of people who share interests and/or activities, or who are interested in exploring the interests and activities of others.

## **National Cyber Alert System**

## “Social networking sites…build on the concept of traditional social networks where you are connected to new people through the people you already know.” “Friend of a Friend”

## **Web 2.0**

## technology that “allows users to interact with others and to change website content, in contrast to non-interactive websites that are limited to passive viewing of information.” (Wikipedia)

## Examples: Social networking sites, video sharing sites, blogs, etc.

## **Facebook** & **Myspace -** Free-access social networking websites

## **Twitter** – “micro” blog – 140 characters or less

## **Blog** – shared on-line journal

## **Video Sharing Sites** – YouTube, Flikr

## **Podcast** – audio broadcast that can be downloaded

**16.2 The Good, the bad and the Ugly**

* **The Good**

## Networking

## Communicating

## Reconnecting with old friends

## Keeping up with family

## Business marketing and promotion

#### i.e., Facebook, Twitter

## Entertaining and fun

# **Virginia Tech Example**

## After shooting rampage in 2007, campus in lockdown mode, phone lines jammed, website overloaded – students, faculty, staff used “…MySpace and Facebook to get in touch with family and friends outside traditional channels.” It was also used to “…send condolences, share memories and gain closure.”

## \*SC Magazine, article “Social Anxiety”, page 21, August 2009.

* **The Bad and the Ugly**

## Personal information could get in the wrong hands. Phishing scams, viruses and spyware may spread through social networks. Once you’ve posted something, others can copy it or it may exist in cache, so that even if you delete it, it may still exist and is out of your control.

## Anti-social? If you spend all your time on the computer

## Internet provides sense on anonymity.

## Lack of physical contact may give false sense of security.

## People may post information for friends to read, forgetting that others may see it.

# **Examples**

## The case of a person asking for emergency money while impersonating a Facebook user to her friends

### http://eliasbizannes.com/blog/2009/01/phishing-for-fraud-on-facebook/

## Also the British MI6 chief that was exposed by his wife’s Facebook pictures:

### http://www.dailymail.co.uk/news/article-1197562/MI6-chief-blows-cover-wifes-Facebook-account-reveals-family-holidays-showbiz-friends-links-David-Irving.html

* **How can you protect yourself?**

### Keep private information private

## Do not post address, ssn, phone number, financial info, your schedule, full birth date

## Be careful not to display information used to answer security questions (e.g., favorite pet, mother’s maiden name)

### Use caution when you click links

### Be careful about installing extras on your site

### Be wary of unknown friends (strangers)

### Google yourself

### Don’t blindly connect

### Trust your gut instinct

### Use and maintain anti-virus software

### Use strong passwords

### Don’t use the same password for a social networking site and for your email

### Remember - social networking sites are a public resource – like a billboard in cyberspace

### Evaluate sites privacy settings

## Lock down your profile information to people you accepts as a friend. That way no one can read your personal information unless they are an approved friend

### Be skeptical

* **Protect your children**

### “It’s 10 p.m., do you know where your children are?”

## “And who they are talking to online?”

### Age limits on some social networking sites

## Facebook and MySpace open to people 13 and older

## Twitter open to all

### Talk to children about online safety. Tell them to keep personal information private. Explain what personal information is (address, ssn, phone number, schedule, birth date, etc.), and to not share personal information of their family or their friends either.

### Caution them about sharing information such as school names, sports teams, where they work, hang out or other info that can be used to identify or locate them offline. Warn them to only be “friends” with people they actually know and are friendly with in real life.

## Talk to them about bullying

## Remind them that once they post information online, just because they delete it, it might not be really gone.

## Warn about dangers of flirting with strangers online. Warn about online sex talk.

## Tell them to trust their gut if suspicious.

### Keep the computer in an open area, like the kitchen or family room.

### Use the Internet with your kids.

## Create a Facebook or MySpace profile

## Be one of their “friends”

## Let your kids know that you are there

## Teach them how to act as they socialize online

### Check their profile

## Check the privacy settings

## Review their list of friends

## Make sure their screen name doesn’t say too much about them. It may be dangerous to use full name, age or hometown.

Lecture 17

Introduction to Hacking

**17.1 What Is Network Security?**

## Security is much larger than just packets, firewalls, and hackers. Security includes:

### Policies and procedures

### Liabilities and laws

### Human behavior patterns

### Corporate security programs and implementation

### Technical aspects- firewalls, intrusion detection systems, proxies, encryption, antivirus software, hacks, cracks, and attacks

## Understanding hacking tools and how attacks are carried out is only one piece of the puzzle.

**17.2 Hacking**

## The process of attempting to gain or successfully gaining, unauthorized access to computer resources for the purpose of help or secure system is called hacking.

* **History of Hacking**

### 1966 – Robert Morris introduces the concept of safe hacking.

### 1969 – Development in the field of hacking.

### 1990 – Electronic frontier foundation was founded.

### 1995 – Mark Andreessen & Eric release mosaic

* **Who is Hacker?**

## Hacker is not cyber-criminal but he is the very intelligent person who uses his knowledge in constructive manner to secure system & never damage data. He knows all about the operating system & different holes in the system.

* **Who is cracker?**

### Person who enter into other’s system and violet the system, damage the data, create havoc is called cracker

### Cracker is cyber criminal

### They can be easily identified because their actions are malicious

* **Why do crackers exist?**

### Crackers exist because human nature is just so, frequently driven by to destroy instead of create

### They are used for different purposes like for profit, some company use them for disabling the competitor company, for cracking credit card number

* **Difference between hacker & cracker**

### Hacker’s programs to check integrity of other programs, thus when hackers create program it automatically checks remote machine security structure

### They always do constructive work

### Crackers rarely make their own program instead, they steal tool, programs from others

### Crackers creates nothing & destroy much

* **Which operating system hacker use**

### Sun

### Unix

### Microsoft

**Sun**

### Hackers use either solaric x86 or sco as a platform.

### This is because these products are licensed ware & they can easily be obtained.

**Unix**

### Popular platform because they required a low overhead

### We can run linux on a paltray 386 and gain good performance.

### This is reasonable.

**Microsoft**

### This supports many security tools that can be used to attack remote machine.

### It has advanced tools for networking as well.

Lecture 18  
Hacking (Continued)

**18.1 Why Do People Hack?**

### Just for fun.

### Show of their knowledge

### Hack other system secretly.

### Destroy enemy’s computer network during the war.

### For profit people pays a cracker.

### Crack for sake of curiosity.

* **The Psychology of Hackers**

### All information should be free.

### Access to computer should be unlimited and free.

### It can change life for better.

### It can create beauty on computer.

**18.2 Types of hacking**

## There are many types of hacking like:

### Password hacking

### Software hacking

### Net hacking

* **Password hacking**

## There are two types for password hacking. Brute force and dictionary based.

## **Brute force**

### In that case hackers try out all the combination of all keyboard letters .it has greater success but it takes long time

## **Dictionary based**

### In that they are use predefine password.it is unsuccessful method

* **Software hacking**

## In that hackers changes the look & execution way of that software

## Change the demo version into full version by decoding the source code

* **IP address**

## IP address is the address of your computer in the internet. It is unique. Like:

## 192.168.23.45

* **Port**

## It is not physical port but it is logical port in your computer. It is just like hole onto the system through hacker can enter. There are thousands of ports into computer. The particular service is running on particular port. Like:

## Port 21: ftp

## Port 23: telnet

## Port 80: http

## Port 25: mail

* **Hacking tools**

## There are many tools are available

## Scanners

## Telnet

## FTP

## LAN watch

* **Scanners**

## It is not a photo scanner. Scanner is program that automatically detects security weakness in remote host. Port scanners are used in hacking. Port scanner can give the whole list of open port on that system and which service is running on that. It can use almost all operating system.

## ex. SATAN,NMAP

* **Telnet**

## Telnet is ultimate hacking tool. It is terminal emulation program that allows us to connect to remote system. You have to follow this step to use telnet.

## C:\windows\telnet [ip address] port

* **Ftp**

## FTP is one type of protocol but some time it is used as hacking tool, port 21 for the ftp. For connecting ftp we need some ftp s/w known as ftp client. For connecting ftp server you have to hammer that server.

## Command: c:\windows\ftp [ip address]

Lecture 19

Introduction to Hacking

**19.1 What Is Network Security?**

## Security is much larger than just packets, firewalls, and hackers. Security includes:

### Policies and procedures

### Liabilities and laws

### Human behavior patterns

### Corporate security programs and implementation

### Technical aspects- firewalls, intrusion detection systems, proxies, encryption, antivirus software, hacks, cracks, and attacks

## Understanding hacking tools and how attacks are carried out is only one piece of the puzzle.

* **Attacks**

## There are many types of attacks

### Spoofing attack

### Telnet based attack

### DOS (Daniel of service) attack

### Ping of death

### Distributed dos attack

### Mail bombs

* **Need For Security**

## Some excellent software can provide you best security, like:

### Trojan

### Firewall

* **Trojan**

## Windows Trojans are small aspect of windows security. Trojan is unauthorized program contained within a legitimate program. This program performs function unknown by user.

* **Firewall**

## Firewall is any device used to prevent outsiders from gaining access to your network. Types of firewalls are:

### Packet filter

### Application proxy

### Packet inspection

**19.2 Common Steps for Attackers**

## Reconnaissance

### Intelligent work of obtaining information either actively or passively

### Examples:

#### Passively: Sniffing Traffic, eavesdropping

#### Actively: Obtaining data from American Registry for Internet Numbers (ARIN), whois databases, web sites, social engineering

## Scanning

### Identifying systems that are running and services that are active on them

### Examples: Ping sweeps and port scans

## Gaining Access

### Exploiting identified vulnerabilities to gain unauthorized access

### Examples: Exploiting a buffer overflow or brute forcing a password and logging onto a system

## Maintaining Access

### Uploading malicious software to ensure re-entry is possible

### Example: Installing a backdoor on a system

## Covering Tracks

### Carrying out activities to hide one’s malicious activities

### Example: Deleting or modifying data in a system and its application logs

**19.3 Where do Attackers get the Most Traction?**

## Flaws within software are the root of the problem of successful attacks and exploits. Security does not like complexity. The more complex software gets, the harder it is to properly predict how it will react in all possible scenarios thus making it much harder to secure. Windows XP is approximately 40 million lines of code. Linux is approximately 2 million lines of code. Estimate in industry: 5 to 10 bugs per 1,000 lines of code => Windows XP has approximately 200,000 bugs.

## With object-oriented language applications and operating systems using each other’s code, DLLs are installed and shared, many applications communicate with each other => Operating Systems cannot control this flow and provide protection against possible compromises

* **Enough Blame to Go Around**

### Software vendors do not consider security in the design and specification phases. Programmers have not been properly taught how to code securely. Vendors are not held liable for faulty code. Consumers are not willing to pay more for properly developed and tested code.

* **Novice versus Advanced**

### Novice ethical hacker will use tools/techniques developed by others. A more advanced ethical hacker will not only depend upon other people’s tools but will have the skill set and understanding to develop their own tools/techniques.

Lecture 20  
Hacking (Continued)

**20.1 Spoofing**

## Definition:

## An attacker alters his identity so that someone thinks he is someone else

### Email, User ID, IP Address,

### Attacker exploits trust relation between user and networked machines to gain access to machines

## Types of Spoofing:

### IP Spoofing:

### Email Spoofing

### Web Spoofing

* **IP Spoofing – Flying-Blind Attack**

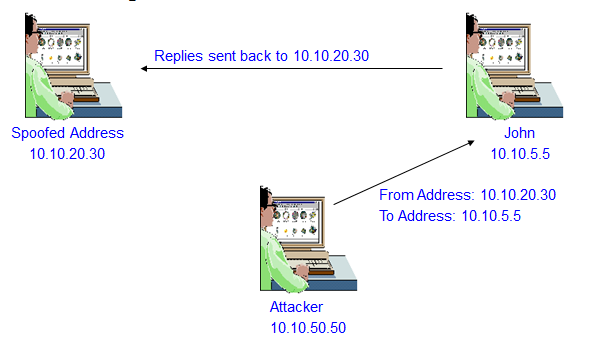
## Definition:

## Attacker uses IP address of another computer to acquire information or gain access

### Attacker changes his own IP address to spoofed address

### Attacker can send messages to a machine masquerading as spoofed machine

### Attacker cannot receive messages from that machine



**Figure 20.1: IP Spoofing – Flying-Blind Attack**

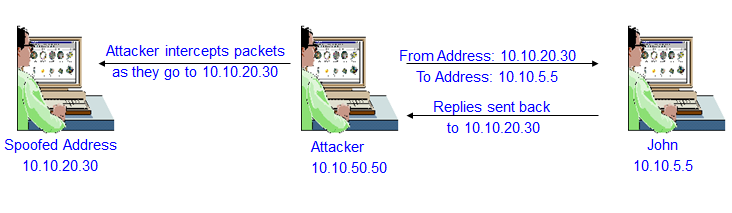
* **IP Spoofing – Source Routing**

## Definition:

## Attacker spoofs the address of another machine and inserts itself between the attacked machine and the spoofed machine to intercept replies.

### The path a packet may change can vary over time

### To ensure that he stays in the loop the attacker uses source routing to ensure that the packet passes through certain nodes on the network



**Figure 20.2: IP Spoofing – Source Routing**

* **What Is E-Mail Spoofing?**

### E-mail spoofing is the falsification of an e-mail [header](http://whatis.techtarget.com/definition/0,,sid9_gci213480,00.html) so that the message appears to have originated from someone or somewhere other than the actual source. Distributors of [spam](http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci213031,00.html) often use spoofing in an attempt to get the recipient to open, and possibly respond to, their solicitations. Spoofing can be used legitimately. Two examples of a sender who might prefer to hide the source of an e-mail is someone reporting mistreatment by a spouse to a welfare agency or a "whistle-blower" who fears retaliation. Spoofing anyone other than you is illegal in some areas.

### Spoofing may occur in different forms, but all have a similar result: a user receives email that seems to have come from one source when it actually was sent from another. Email spoofing is often an attempt to trick the user into making a damaging statement or giving out sensitive information (such as passwords).

### Examples of spoofed email that could potentially affect you include:

### Email claiming to be from a system administrator requesting users to change their passwords to a specified string and threatening to suspend their account if they do not do this

### Email claiming to be from a person in authority requesting users to send them a copy of a password file or other sensitive information

### Although most spoofed e-mail falls into the "annoyance" category and requires little action other than deletion, the more malicious varieties can cause serious problems and security risks. For example, spoofed e-mail may claim to be from someone in a position of authority, asking for sensitive data, such as passwords, credit card numbers, or other personal information -- any of which can be used for a variety of criminal purposes. The Bank of America, eBay, and Wells Fargo are among the companies recently spoofed in mass spam mailings.

### The best form of defense is a good offense.  Delete suspicious e-mail without opening attachments or clicking links.

## **Types of Email Spoofing:**

## Create an account with similar email address

### Sanjaygoel@yahoo.com: A message from this account can perplex the students

## Modify a mail client

### Attacker can put in any return address he wants to in the mail he sends

## Telnet to port 25

### Most mail servers use port 25 for mails. Attacker logs on to this port and composes a message for the user.

* **Web Spoofing**

## Basic

### Attacker registers a web address matching an entity e.g. votebush.com, geproducts.com, gesucks.com

## Man-in-the-Middle Attack

### Attacker acts as a proxy between the web server and the client

### Attacker has to compromise the router or a node through which the relevant traffic flows

## URL Rewriting

### Attacker redirects web traffic to another site that is controlled by the attacker

### Attacker writes his own web site address before the legitimate link

## Tracking State

### When a user logs on to a site a persistent authentication is maintained

### This authentication can be stolen for masquerading as the user

# **Web Spoofing – Tracking State**

## Web Site maintains authentication so that the user does not have to authenticate repeatedly

## Three types of tracking methods are used:

### Cookies: Line of text with ID on the users cookie file

### Attacker can read the ID from users cookie file

### URL Session Tracking: An id is appended to all the links in the website web pages.

### Attacker can guess or read this id and masquerade as user

### Hidden Form Elements

### ID is hidden in form elements which are not visible to user

### Hacker can modify these to masquerade as another user

**20.2 Session Hijacking**

## Definition:

## Process of taking over an existing active session

## Modus Operandi:

### User makes a connection to the server by authenticating using his user ID and password.

### After the users authenticate, they have access to the server as long as the session lasts.

### Hacker takes the user offline by denial of service

### Hacker gains access to the user by impersonating the user

# 

**Figure 20.3: Session Hijacking**

## Attacker can

### Monitor the session

### Periodically inject commands into session

### Launch passive and active attacks from the session

* **Session Hijacking – How does it Work?**

## Attackers exploit sequence numbers to hijack sessions. Sequence numbers are 32-bit counters used to:

### Tell receiving machines the correct order of packets

### Tell sender which packets are received and which are lost

## Receiver and Sender have their own sequence numbers. When two parties communicate the following are needed:

### IP addresses

### Port Numbers

### Sequence Number

## IP addresses and port numbers are easily available so once the attacker gets the server to accept his guesses sequence number he can hijack the session.

**20.3 Denial of Service (DOS) Attack**

## Definition:

## Attack through which a person can render a system unusable or significantly slow down the system for legitimate users by overloading the system so that no one else can use it.

## Types:

## Crashing the system or network

### Send the victim data or packets which will cause system to crash or reboot.

## Exhausting the resources by flooding the system or network with information

### Since all resources are exhausted others are denied access to the resources

## Distributed DOS attacks are coordinated denial of service attacks involving several people and/or machines to launch attacks.

## **DOS Types:**

### Ping of Death

### SSPing

### Land

### Smurf

### SYN Flood

### CPU Hog

### Win Nuke

### RPC Locator

### Jolt2

### Bubonic

### Microsoft Incomplete TCP/IP Packet Vulnerability

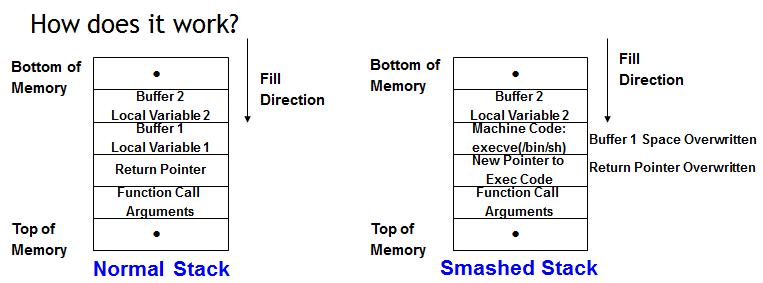
### HP Openview Node Manager SNMP DOS Vulneability

### Netscreen Firewall DOS Vulnerability

### Checkpoint Firewall DOS Vulnerability

* **Buffer Overflow Attacks**

## This attack takes advantage of the way in which information is stored by computer programs. An attacker tries to store more information on the stack than the size of the buffer.



**Figure 20.4: Buffer Overflow Attacks**

## **How does it work?**

## Programs which do not do not have a rigorous memory check in the code are vulnerable to this attack

## Simple weaknesses can be exploited

### If memory allocated for name is 50 characters, someone can break the system by sending a fictitious name of more than 50 characters

## Can be used for espionage, denial of service or compromising the integrity of the data

## Examples

### NetMeeting Buffer Overflow

### Outlook Buffer Overflow

### AOL Instant Messenger Buffer Overflow

### SQL Server 2000 Extended Stored Procedure Buffer Overflow

Lecture 21  
Computer Security Ethics

**21.1 Introduction**

## Being ethical is not necessarily following one’s feelings; “feelings frequently deviate from what is ethical“. Often because of the way one is raised, ethics and religion are coupled; but ethics is not confined to religion nor is the same as religion. Being ethical is not solely following the law.

## Elements of practical ethics through basic philosophy:

### Ethical thought

### Ethical definition

### Ethical values

## Example: “If a person conceives of engineering activity as only making money, then one's definition of practical ethics, one's actions and values will, be guided by this basic philosophical position. “

## **Security in:**

### Client / Workstation / Terminal

### Intra-networks

### Inter-networks

## **In terms of:**

### Physical Security

### Non-Physical Security

## **Security Threats (sources, causes, people behind):**

### Hackers

### Crackers

### Script Kiddies

### Unethical Employees (logic bombs, backdoor,…)

### Cyberterrorists

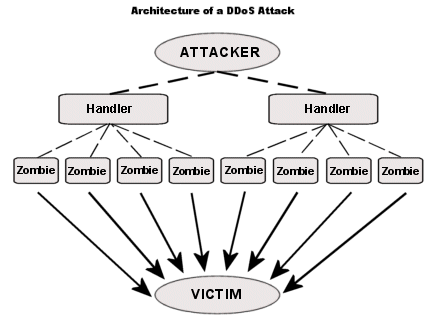
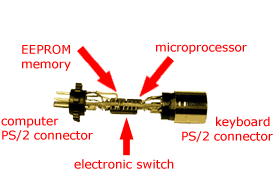
### Corporate Spy

### Worm / Virus / Trojan (incl. keyloggers,…)

### Spoofing / Sniffing / Phishing

### DoS / DDoS attacks

**Examples:**

****

# **Example of Phishing:**

# 

**21.2 Hackers’ Code of Ethics:**

## Hacker creed (Steven Levy’s “Hackers: Heroes of Computer Revolution” - 1984 ):

## Access to computers should be unlimited and total.

## Always yield to the Hands-On Imperative

## All information should be free.

## Mistrust authority -- promote decentralization.

## Hackers should be judged by their hacking.

## You can create art and beauty on a computer.

## Computers can change your life for the better.

## New Code of Ethics (90s) - Steven Mizrach :

## "Above all else, do no harm"

## Protect Privacy

## "Waste not, want not."

## Exceed Limitations

## The Communicational Imperative

## Leave No Traces

## Share!

## Self Defense

## Hacking Helps Security

## Trust, but Test!

## In Short : 1) protect data and hardware 2) respect and protect privacy 3) utilize what is being wasted by others 4) exceed unnecessary restrictions 5) promote peoples' right to communicate 6) leave no traces 7) share data and software 8) be vigilant against cyber-tyranny and 9) test security and system integrity of computer systems.

* **New(er) Hacker Ethics:**

## Hackers share and are willing to teach their knowledge. Hackers are skilled. Many are self-taught, or learn by interacting with other hackers. Hackers seek knowledge. This knowledge may come from unauthorized or unusual sources, and is often hidden. Hackers like to understand how things work, and want to make their own improvements or modifications.

## Hackers often disagree with authority, including parents, employers, social customs and laws. They often seek to get around authority they disagree with. Hackers disagree with each other. Different hackers have different values, and come from all backgrounds. This means that what one hacker is opposed to might be embraced by another.

## Hackers are persistent, and are willing to devote hours, days and years to pursuing their individual passions. This Code is not to prescribe how hackers act. Instead, it is to help us to recognize our own diversity and identity.

## Every hacker must make his or her own decisions about what is right or wrong, and some might do things they believe are illegal, amoral or anti-social.

## Hackers' motivations are their own, and there is no reason for all hackers to agree. Hackers have a shared identity, however, and many shared interests. By reading this Code, hackers can recognize themselves and each other, and understand better the group they are a part of.

* **Hackers’ Code of Ethics:**

## Old code vs new code

## Are new hackers aware of the original hacker ethics?

## Are new hackers aware of any hacker ethics?

## Influence of technology and social issues on changes in hacker ethics

## Similarity between the old and new ethics and ethical continuity

**21.3 Ethical Issues in Security Courses**

## More security subjects are moved from graduate level to undergraduate level; graduate students are more mature than undergraduate ones. Are security courses’ materials really appropriate? (Some include: trying DDOS, writing and spreading a virus,…)

## Major of computer hackers are under the age of 25 and many of them are college students. Using hacking tools in labs and classes increases “comfort level” with such tools 🡪 the more comfortable people become with one computer technology, the more likely they are to use them

## There are many justifications for teaching such sensitive issues: to strengthen the nation’s defense against attacks. But do we need to know the details of how to make a bomb in order to defend ourselves against bomb attacks? Using password crackers is not necessary to teach the dangers of using weak and insecure passwords.

## “Students would learn them on their own anyway. We are presenting this material in a responsible manner.” The big question is: how to really present this material in a responsible manner?

## Requiring students to sign a statement and take an ethical oath? Teaching ethical issues as part of a course? Problem: ethical standards cannot be integrated in individuals just over a short period of time!

## Ethical subjects are necessary especially in computer security curricula. Ethical standards should be taught to students early in the program and students should be reminded of them throughout the program.

## Students should become aware about the consequences of misuse of their knowledge

## The problem of “deindividualism” (group size, anonymity)

## “Deindividualism is a feeling of separation and anonymity that can lead to individuals engaging in a broader range of unethical behaviors.”

## “Deindividuation is the psychological state of separation of the individual from others”. It is often seen in chat rooms and message boards.

## Making students aware that they are trusted with something important encourages them to live up to that trust.

## Sensitive topics should be taught and discussed at higher levels of a program.

Lecture 22  
Ethical Hacking

**22.1 Hacker and Ethical hacker**

## Hackers

### Access computer system or network without authorization

### Breaks the law; can go to prison

## Ethical hacker

### Performs most of the same activities but with owner’s permission

### Employed by companies to perform penetration tests

* **Penetration test vs. Security test**

## Penetration test

### Legal attempt to break into a company’s network to find its weakest link

### Tester only reports findings

## Security test

### More than an attempt to break in; also includes analyzing company’s security policy and procedures

### Tester offers solutions to secure or protect the network

## Programming languages used by experienced penetration testers

### Practical Extraction and Report Language (Perl)

### C

### Tiger box

### Collection of OSs and hacking tools

### Helps penetration testers and security testers conduct vulnerabilities assessments and attacks

* **Penetration-Testing Methodologies**

## Penetration-Testing Methodologies

### White box model

### Black box model

### Gray box model

## White box model

### Tester is told everything about the network topology and technology

### Tester is authorized to interview IT personnel and company employees

### Makes tester job a little easier

## Black box model

### Company staff does not know about the test

### Tester is not given details about the network

### Burden is on the tester to find these details

### Tests if security personnel are able to detect an attack

## Gray box model

### Hybrid of the white and black box models

### Company gives tester partial information

* **Certification Programs for Network Security Personnel**

## Penetration testers need to have

### The technical skills

### Good understanding of networks

### The role of management in an organization

## Network security certification programs

### Certified Ethical Hacker (CEH)

### OSSTMM Professional Security Tester (OPST)

### Certified Information Systems Security Professional (CISSP)

### Global Information Assurance Certification (GIAC)

## Certifications that help prepare for these certifications

### CompTIA Security+

### Network+

**22.2 Certified Ethical Hacker (CEH)**

## Developed by the International Council of Electronic Commerce Consultants (EC-Council)

### Based on 21 domains (subject areas)

### Web site: www.eccouncil.org

### Red team: Composed of people with varied skills

### Conducts penetration tests

### **OSSTMM Professional Security Tester (OPST)**

## Designated by the Institute for Security and Open Methodologies (ISECOM)

### Based on the Open Source Security Testing Methodology Manual (OSSTMM)

### Consists of 5 domains

### Web site: www.isecom.org

### **Certified Information Systems Security Professional (CISSP)**

## Issued by the International Information Systems Security Certifications Consortium (ISC2)

### Usually more concerned with policies and procedures

### Consists of 10 domains

### Web site: www.isc2.org

**22.3 SANS Institute**

## SANS Institute provides a set of computer security certifications linked to the training courses provided by the SANS. GIAC is specific to the leading edge technological advancement of IT security the SANS organization changed the format of the certification by breaking it into two separate levels. The "silver" level certification requires two multiple-choice tests, whereas the "gold" level certification has both the multiple-choice tests requirement as well as a practical.

## SysAdmin, Audit, Network, Security (SANS).

### Offers certifications through Global Information Assurance Certification (GIAC)

### Top 20 list

### One of the most popular SANS Institute documents

### Details the most common network exploits

### Suggests ways of correcting vulnerabilities

### Web site: www.sans.org

**22.4 What You Can Do Legally**

## As an ethical hacker, be aware of what is allowed and what is not allowed

### Laws involving technology change as rapidly as technology itself

### Find what is legal for you locally

### Laws change from place to place

## Some hacking Tools on your computer might be illegal to possess

### Contact local law enforcement agencies before installing hacking tools

## In UK and Germany, using or writing real hacking tools like Nessus, Metasploit, Hydra, Amap, John, other exploits are fairly telltale illegal.

## Some people against this idea claim that “If you own a crow bar, a favored tool for breaking through locked doors, that’s fine. If you own a baseball bat, a wonderful tool which many put to use bashing in people’s skulls, that’s fine. Own a piece of software that can port scan, and you break the law.”

* **Is Port Scanning Legal?**

## Federal Government does not see it as a violation

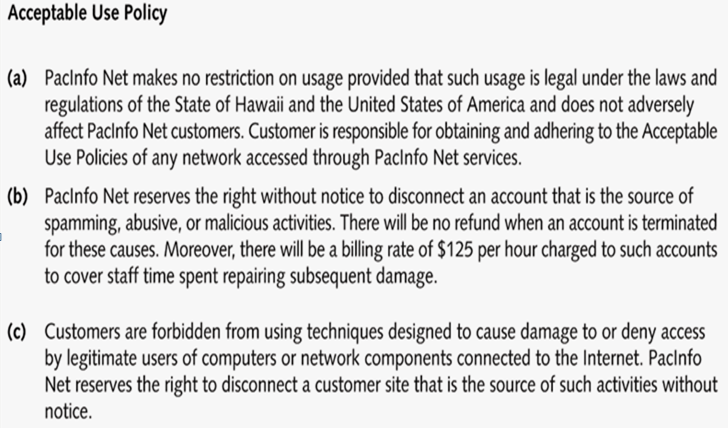
### Allows each state to address it separately

### Some states deem it legal

### As noninvasive or nondestructive in nature

### Not always the case

## Read your ISP’s “Acceptable Use Policy”



**Figure 22.1: An Example of Acceptable Use Policy**

* **Federal Laws**

## Federal computer crime laws are getting more specific

### Cover cybercrimes and intellectual property issues

## Computer Hacking and Intellectual Property (CHIP)

### New government branch to address cybercrimes and intellectual property issues

**22.5 What You Cannot Do Legally**

## Accessing a computer without permission is illegal. Other illegal actions

### Installing worms or viruses

### Denial of Service attacks

### Denying users access to network resources

## As an independent contractor (ethical hacker), using a contract is just good business

### Contracts may be useful in court

### Internet can also be a useful resource

### Have an attorney read over your contract before sending or signing it

# **Ethical Hacking in a Nutshell**

## What it takes to be a security tester?

### Knowledge of network and computer technology

### Ability to communicate with management and IT personnel

### Understanding of the laws

### Ability to use necessary tools

Lecture 23 & 24  
Plagiarism and Referencing

**23.1 What is plagiarism?**

## Plagiarism can be defined as ‘Plagiarism is passing off someone else’s work, whether intentionally or unintentionally, as your own for your own benefit’ (Carroll, 2002, p.9).

## **Examples of plagiarism**

### Using a direct quote without referencing

### Using someone else’s ideas or words without referencing

### Paraphrasing work by only changing a few words

### Using lecture/tutorial notes without referencing

### Copying another person’s work and submitting it as your own

### Submitting another person’s work in whole or in part

### Submitting work that has been written by someone else on your behalf

### Colluding when two or more students submit identical work (Bretag, Crossman & Bordia, 2006)

* **Different Terminologies**

## **Terminology: Copyright**

## Copyright is "a form of protection provided by a government to the authors of 'original works of authorship,' including literary, dramatic, musical, artistic, and certain other intellectual works. This protection is available to both published and unpublished works."

## **Terminology: Fair Use**

## Fair Use is a statute under copyright law that allows for the use of limited portions of a work that has copyright without having to have permission from the original author. It was created for the purposes of education and research. It’s a little harder to pin down than plagiarism or copyright. I mean, what qualifies as a "limited portion"?

## The Copyright Office isn't very helpful on defining what a "limited portion" is. It only states that "there is no specific number of words, lines, or notes that may safely be taken without permission." When using someone else's work, it's best to always give credit where credit's due, even if using only a small part. If you're unsure, then ask for permission.

* **Legal Implications**

## Is it against the law?

## How is it applied at the college level?

### Most schools and universities have policies on cheating and plagiarism.

## Majority of universities have following policy:

### First offense: failing grade on assignment

### Second offense: failing grade for the course

### Third offense: suspension

# What are the purposes of referencing?

### To avoid plagiarism

### To add strength and credibility as evidence to support your position

### To indicate scope and depth of your research

### To allow others to follow up content presented independently

# What should be referenced?

### Everything that is not your own original idea

### Quotes

### Paraphrases

### Summaries

### Statistical information

### Diagrams/tables/graphs/images

* **Harvard Referencing System (Journal Article)**

### In text: (Author’s surname, Year, Page number if required)

### E.g. (Guthrie, Petty & Ricceri, 2006, p. 256)

### Reference list: Author’s surname, First initial (Year) ‘Title of article’, Name of Journal, volume, number, range of pages.

### E.g. Guthrie, J, Petty, R & Ricceri, F (2006), ’The voluntary reporting of intellectual capital. Comparing evidence from Hong Kong and Australia’, Journal of Intellectual Capital, vol. 7, no. 2, pp.254-271.

* **Harvard Referencing System (books)**

## 

### In text: (Author’s surname, Year, Page number if required)

### E.g. (Watts & Zimmerman, 2006, p. 61)

### Reference list: Author’s surname, First initial, (Year), Name of book, Publisher, Place of Publication.

### E.g. Watts, R & Zimmerman, J, (2006), Positive Accounting Theory, Prentice-Hall, Englewood Cliffs, NJ.

* **Quote**

## Because ‘[t]he annual report is the most efficient way for an organisation to communicate with those stakeholder groups deemed to have an interest in controlling certain strategic aspects of an organisation’ (Guthrie, Petty & Ricceri, 2006, p. 256), it is critical that….

* **Paraphrase**

## In communicating with stakeholders interested in exerting influence in areas of strategy, the annual report serves as the best means for the organisation to achieve this (Guthrie, Petty & Ricceri, 2006, p. 256).

* **Quote or paraphrase across two pages**

## The industry classifications used in the Hong Kong study consisted of: ‘consolidated enterprises, finance, hotels, general industry, and property, utilities and growth enterprise’ (Guthrie, Petty & Ricceri, 2006, pp. 262-263).

* **Summary**

## Guthrie, Petty and Ricceri (2006) explain how the stakeholder and legitimacy theories make use of content analysis, such as in relation to annual reports.

* **Statistical information**

## This was based on information from the financial year ending 30 June 1998 (Guthrie, Petty & Ricceri, 2006, p. 258).

* **Secondary Reference**

## When you use author A’s work that is cited in author B, both authors are cited in-text.

## A student might write the following:

## E.g. the ethical branch of the stakeholder theory argues that all stakeholders must be treated fairly, no matter their level of power (Deegan, 2000 in Guthrie et al., 2006, p. 256).

## Only author B is acknowledged in the reference list:

## E.g. Guthrie, J, Petty, R & Ricceri, F (2006), ’The voluntary reporting of intellectual capital. Comparing evidence from Hong Kong and Australia’, Journal of Intellectual Capital, vol. 7, no. 2, pp.254-271.

* **When is the page number required in the in text reference?**

### Specific information from a specific page

### Specific information from across two pages

### Statistics/ diagrams/ tables

* **Referencing Government or Standards Publications**

## Due to differences in form/publisher, sometimes additional relevant details are required to ‘pinpoint’ location of information:

## In text: (AASB, 2007, AASB 2, para. 19)

## Reference list: AASB (Australian Accounting Standards Board), 2007, AASB 2 Share-based Payments, AASB, Canberra, viewed 7 May 2008 <http://www.aasb.com.au>.

* **Which should you rely on most: quoting or paraphrasing? Why?**

## Paraphrasing

### Shows understanding of what you have read

### Allows integration of source information into your own argument more easily

## Quoting – use only if:

### Paraphrasing causes misinterpretation

### Analysing the quote itself is important

### Exact words from the source are particularly forceful

* **Common Errors in Referencing**

### No reference provided where necessary

### Reference provided where not necessary

### Incorrect source provided as reference

### Quotation marks not used where necessary

### Page numbers not included where necessary

### Incorrect page numbers given

### Use of page number instead of paragraph number in references to Government or Standards publications

### Misspelling

### Incorrect/inconsistent punctuation

* **Placement of in text reference**

## After specific information in part of sentence or at end of sentence, when reading, look for language structures associated with use of sources:

### X is considered a component of…;

### Y is claimed to be…

### The term Z refers to…

### Several studies have revealed that…

* **How to avoid plagiarism**

### Read like a writer

### Take note of sources while researching

### Paraphrase while taking notes

### Reference appropriately

### Manage time

Lecture 25  
Referencing

**25.1 Introduction**

* **In-Text Referencing Systems**

## In text reference e.g. Davis and McKay (1996, p.112) note that “it is important to be flexible about the system of referencing and adopt whichever style is appropriate”.

## Full reference e.g. Davis, L.B. and McKay, S. 1996, Structures and Strategies: An introduction to Academic Writing, Macmillan Education Australia, Melbourne.

* **Number-Note Referencing Systems**

## Numbered reference Davis and McKay note that “it is important to be flexible about the system of referencing and adopt whichever style is appropriate” [1].

## Full reference: Lloyd Davis and Susan McKay, Structures and Strategies: An introduction to Academic Writing, Macmillan Education Australia, Melbourne, 1996, p.112.

**25.2 Types of Referencing**

## There are a few main types of referencing: H**arvard** (mostly used by Social Sciences, Business, Engineering and Science), **Oxford and Cambridge** (mostly used in Law subjects and occasionally referred to as 'footnoting') and **APA** (American Psychological Association (Psychology and some Health Science areas) – but there are also others.

**1. In-Text Referencing Systems**

* **Harvard system**

## In text reference: Davis and McKay (1996, p.112) note that it is important to be flexible about the system of referencing and adopt whichever style is appropriate.

## Full reference: Davis, L.B. and McKay, S. 1996, Structures and Strategies: An introduction to Academic Writing, Macmillan Education Australia, Melbourne.

* **APA system**

## In text reference Davis and McKay (1996) note that it is important to be flexible about the system of referencing and adopt whichever style is appropriate (p.112).

## Full reference: Davis, L.B. & McKay, S. 1996, Structures and Strategies: An introduction to Academic Writing, Melbourne: Macmillan Education Australia.

* **MLA system**

## In text reference: Davis and McKay note that it is important to be flexible about the system of referencing and adopt whichever style is appropriate (112).

## Full reference: Davis, Lloyd and Susan McKay. Structures and Strategies: An introduction to Academic Writing. Melbourne: Macmillan Education Australia, 1996.

**2. Number-Note Referencing Systems**

## OXFORD SYSTEM Numbered reference: Davis and McKay note that it is important to be flexible about the system of referencing and adopt whichever style is appropriate [1].

## Full reference: Lloyd Davis and Susan McKay, Structures and Strategies: An introduction to Academic Writing, Macmillan Education Australia, Melbourne, 1996, p.112.

## VANCOUVER SYSTEM Numbered reference: Davis and McKay note that it is important to be flexible about the system of referencing and adopt whichever style is appropriate1.

## Full reference: Davis, L.B. & McKay, S. Structures and Strategies: An introduction to Academic Writing, Melbourne: Macmillan Education Australia, 1996

## CAMBRIDGE FOOTNOTING REFERENCE Numbered reference: Davis and McKay note that it is important to be flexible about the system of referencing and adopt whichever style is appropriate1.

## Full reference: (appears at the bottom of the page) 1.Lloyd Davis and Susan McKay. Structures and Strategies: An introduction to Academic Writing. Macmillan.

* **Harvard Referencing – Citing In Text**

## It is the most widely used system in business disciplines. It is the standard in La Trobe University Business subjects. In-text references for a paraphrase\* require:

## 1. Authors Surname (s)

## 2. A comma

## 3. Year of Publication

## When you are taking notes, you should record not only the main points of the author’s work, but also your initial critical evaluation of the material (Davis & McKay, 1996).

## No author? Use the the name of the Institution eg: La Trobe University

## \* PARAPHRASE is when you re-word the writers words (same idea but different words)

**25.3 Works Cited**

## **BOOK WITH 1 AUTHOR:**

### Mumford, Lewis. The Culture of Cities. New York: Harcourt, 1938. Print.

## **BOOK WITH 2 OR 3 AUTHORS:**

### Francis, R. Douglas, Richard Jones, and Donald B. Smith. Destinies: Canadian History since Confederation. Toronto: Harcourt, 2000. Print.

## **BOOK WITH 4 OR MORE AUTHORS:**

### Baldwin, Richard et al. Economic Geography and Public Policy. Princeton: Princeton UP, 2003. Print.

## **TWO OR MORE BOOKS BY THE SAME AUTHOR:**

### Replace the author's name by three hyphens and arrange alphabetically by the book's title:

### Postman, Neil. Amusing Ourselves to Death: Public Discourse in the Age of Show Business. New York: Viking, 1985. Print.

### The Disappearance of Childhood. New York: Vintage, 1994. Print.

## **ANTHOLOGY OR COMPILATION:**

### Abate, Corinne S., ed. Privacy, Domesticity, and Women in Early Modern England. Burlington, VT: Ashgate, 2003. Print.

## **A WORK IN AN ANTHOLOGY OR AN ESSAY IN A BOOK:**

### Naremore, James. "Hitchcock at the Margins of Noir." Alfred Hitchcock: Centenary Essays. Ed. Richard Allen and S. Ishii-Gonzalès. London: BFI, 1999. 263-77. Print.

## **BOOK BY A CORPORATE AUTHOR:**

### Associations, corporations, agencies and organizations are considered authors when there is no single author. Organization for Economic Co-operation and Development. Action against Climate Change: The Kyoto Protocol and Beyond. Paris: OECD, 1999. Print.

## **ARTICLE IN A REFERENCE BOOK OR AN ENTRY IN AN ENCYCLOPEDIA:**

### If the article/entry is signed, include the author's name; if unsigned, begin with the title of the entry

### Guignon, Charles B. "Existentialism." Routledge Encyclopedia of Philosophy. Ed. Edward Craig. 10 vols. London: Routledge, 1998. Print.

## **ARTICLE REPRINTED IN A REFERENCE BOOK ONLINE:**

### Carlson, Eric W. “The Range of Symbolism in Poetry.” The South Atlantic Quarterly 48.3 (1949): 442-52. Rpt. in Poetry Criticism. Ed. Jane Kelly Kosek and Christine Slovey. Vol. 13. Detroit: Gale, 1995. 83-84. Literature Criticism Online. Web. 18 Oct. 2009.

## **A TRANSLATION:**

### Kafka, Franz. Metamorphosis. Trans. and Ed. Stanley Corngold. New York: Bantam, 1972. Print.

## **A GOVERNMENT PUBLICATION:**

### United Nations. Dept. of Economic and Social Affairs. Population Division. Charting the Progress of Populations. New York: UN, 2000. Print.

Lecture 26  
Referencing (Continued)

**26.1 Works Cited**

## **BOOK IN A SERIES:**

## Bloom, Harold, Modern Critical Views ed. André Malraux. New York: Chelsea House, 1988

## **ARTICLE IN A JOURNAL:**

## Article retrieved in print/paper format

## Ferrer, Ada. "Cuba 1898: Rethinking Race, Nation, and Empire." Radical

## History Review 73 (1999): 22-49. Print.

## Article retrieved on the Web

## Sehmby, Dalbir S. "Wrestling and Popular Culture." CCLWeb: Comparative Literature and Culture 4.1 (2002): n. pag. Web. 29 Mar. 2009.

## Article retrieved in a library database

## Brennan, Katherine Stern. "Culture in the Cities: Provincial Academies during the Early Years of Louis XIV's Reign." Canadian Journal of

## History 38.1 (2003): 19-42. CBCA Complete. Web. 29 Mar. 2004.

## **ARTICLE IN A NEWSPAPER OR MAGAZINE:**

## Semenak, Susan. "Feeling Right at Home: Government Residence Eschews Traditional Rules." Montreal Gazette 28 Dec. 1995, Final Ed.: A4. Print.

## **AN ENTIRE WEB SITE:**

## Linder, Douglas O. Famous Trials. Univ. of Missouri Kansas-City Law School, 2009. Web. 29 Apr. 2009.

## **A PAGE ON A WEB SITE:**

## An entry for a non-periodical item found on the Web contains the following:

## Last name, First name. "Document title if available." Title of the overall Web site. Version or edition if available. Publisher or N.p. to designate no publisher, publication date or n.d. to mean no date. Web. Date of access.

## "Joyce Wieland." Celebrating Women's Achievements: Women Artists in Canada. National Library of Canada, 2000. Web. 29 Mar. 2004.

## **A REVIEW:**

## Kirn, Walter. "The Wages of Righteousness." Rev. of Cloudsplitter, by Russell Banks. New York Times Book Review 22 Feb. 1998: 9. Print.

## **TELEVISION OR RADIO PROGRAM:**

## "Scandal of the Century." Narr. Linden MacIntyre. The Fifth Estate. CBC Television. 23 Jan. 2002. Television.

## **SOUND RECORDING:**

## Ellington, Duke. "Black and Tan Fantasy." Music is My Mistress. Musicmasters, 1989. CD.

## **FILM, VIDEORECORDING OR DVD:**

## The Shining. Dir. Stanley Kubrick. Perf. Jack Nicholson, Shelley Duvall. Warner Bros., 1980. Videocassette.

## **MUSICAL COMPOSITION PUBLISHED SCORE:**

## Beethoven, Ludwig van. Symphony no. 4 in B-flat major, op. 60. Mineola, NY: Dover, 2001. Print.

## **WORK OF ART, PHOTOGRAPHED, IN A BOOK:**

## Cassatt, Mary. Mother and Child. 1890. Wichita Art Museum, Wichita. American Painting: 1560-1913. By John Pearce. New York: McGraw, 1964. Slide 22.

**26.2 What is the Vancouver Referencing Technique?**

## A uniform set of requirements for bibliographic references. A "numbered" style follows rules established by the International Committee of Medical Journal Editors. It is also known as: Uniform Requirements for Manuscripts Submitted to Biomedical Journals.

## **About Vancouver**

## Small group of editors met in Vancouver, Canada in 1978. Known as Vancouver group Established guidelines for format of manuscripts submitted to their journals. Guidelines developed by the NLM, first published in 1979. Group expanded to International Committee of Medical Journal Editors (ICMJE). ICMJE broadened concerns to include ethical principles related to publication in biomedical journals

## Revised on a regular basis – most recent revision is 2005. ICMJE still operates as a small working group. Most biomedical and IT-related journals today use Vancouver. Vancouver -accredited journals are encouraged to state the use of the technique in their *Instructions to Authors.*

## **In-text Citing**

## A number is allocated to a source in the order in which it is cited in the text. If the source is referred to again, the same number is used. Example: as one author has put it "the darkest days were still ahead" [1]: which is well documented in the literature. [2-5]. this proves that "the darkest days were still ahead". [1]

## **References**

## References are listed in numerical order in the Reference List at the end of the paper

## **Example:**

## 1. Smith SD, Jones, AD. Organ donation. N Engl J Med. 2001;657:230-5.

## 2. Brown JG. Asphyxiation. Med J Aust. 2003; 432:120-4

## **Essential Elements for referencing books**

### Author

### Title

### Edition

### Place of Publication

### Publisher

### Date (year)

## **Examples**

### Personal Author: Adam RD, Victor M. Principles of Neurology. 5th ed. New York: McGraw-Hill, 1993.

### Editor(s) or Compiler(s): Diener HC, Wilkinson M, editors. Drug-induced headache. New York: Springer-Verlag, 1988.

### Organization as author: Virginia Law Foundation. The Medical and legal implications of AIDS. Charlottesville: The Foundation, 1987.

### Chapter in a book: Wynick D, Bloom SR. Islet cell tumors. In: Grossman A. Clinical Endocrinology. Oxford: Blackwells Scientific Publications, 1992: 502-511.

### Conference Proceedings: Preston D, editor. Computers in Clinical Dentistry. Proceedings of the first International Conference on Computers in Clinical Dentistry; 1991 Sept 26-29: Houston. Chicago: Quintessence, 1993.

### Monograph in electronic format: CDI, Clinical dermatology illustrated [monograph on CD-Rom]. Reeves JRT, Maibach H. CMEA Multimedia Group, Producers. 2nd ed. Version 2.0. San Diego: CMEA; 1995.

## **Essential Elements for referencing journals**

### Author

### Title of Article

### Journal Title

### Date

### Volume number

### Issue number

### Page numbers

## **Examples**

(Titles of Journals should be abbreviated according to Index Medicus)

Standard Journal Article: *(list all authors, but if there are more than six, only list the first six followed by “et al”)*

Burks RT, Morgan J. Anatomy of the lateral ankle ligaments. Am J Sports Med 1994 Jan-Feb; 22(1): 72-77.

Organization as author: NIH Technology Assessment Workshop Panel. The Persian Gulf Experience and Health. JAMA 1994; 272: 391-395.

No author given: Coffee drinking and cancer of the pancreas [editorial] BMJ 1981; 283:628.

Volume with supplement: Leff J. Working with the families of schizophrenic patients. Br J Psychiatry 1994; 164 Suppl 23: 71-76.

Issue with supplement: Hirschfeld RMA, Holzer CE. Depressive personality disorders: clinical implications. J Clin Psychiat 1994 Apr; 55 (4Suppl): 10-17.

Journal article in Electronic format: Morse SS. Factors in the emergence of infectious diseases. Emerg Infect Dis [serial online] 1995 Jan-Mar [cited 1996 Jun 5]; 1(1): [24 screens]. Available from: URL: http://www.cdcgov/ncidod/EID/eid.htm

Lecture 27  
Intellectual Property

**27.1 Introduction**

## Intellectual Property simply defined is any form of knowledge or expression created with one's intellect. It includes such things as inventions; computer software; trademarks; literary, artistic, musical, or visual works; and even simply know-how. There are various forms of statutory protection for Intellectual Property, but the two that are most likely to be relevant in the University environment are copyright and patents.

* **Copyright**

## The exclusive right of the holder to copy a creative work or allow someone else to do so, including the sole right to publish, produce or reproduce, to perform in public, to communicate a work to the public by telecommunication, to translate a work, and in some cases, to rent the work.

## Does not protect ideas, but rather the *expression* of such ideas

## Protects original literary, musical, dramatic, or artistic works in a variety of forms, including written materials and computer software comes into existence automatically when the work is created and lasts for the author’s lifetime plus 50 years

## The author of a work is the first owner of copyright; however where a work is created by an employee in the course of his or her employment, in the absence of an agreement to the contrary, the employer is the first owner of the copyright.

* **Patents**

## Protects inventions, which are defined as “any new and useful art, process, machine, manufacture, or composition of matter, or any new and useful improvement in any art, process, machine, manufacture, or composition of matter”

## A Patent prevents anyone else from using the invention without permission for approximately 20 years. After the patent expires, anyone is able to use the invention.

## In order to be patentable, an invention must be novel, and it must have utility and must not be obvious to a person skilled in the field of the invention.

## What makes an invention "new" is that it has not been disclosed publicly prior to the filing of a patent application. If, before that filing, it has been disclosed in an article, a seminar or even in a conversation not covered by a confidentiality agreement, or in confidential circumstances, it will not qualify for a patent in most countries.

* **Know How/Trade Secrets**

## Is special knowledge of how to do something; skill in a particular field.

## Can often have considerable value

## Can be licensed independently and the license need not be restricted to the term of the related patent.

## To protect its commercial value, the owner may wish to keep know-how a trade secret.

## Unlike other forms of intellectual property trade secrecy is basically a do-it-yourself form of protection. The owner doesn't register with the government to secure a trade secret; he or she simply keeps the information confidential. Protection ends when a trade secret is made available to the public.

* **The Clause……**

## Intellectual Property: The University shall own all intellectual property, including technical information, know-how, copyrights, models, drawings, specifications, prototypes, inventions and software developed by University personnel in performance of the Project (“Intellectual Property”). The Company shall have the first option on an exclusive or non-exclusive licence to commercially exploit the Intellectual Property on terms (including compensation to the University) that generally reflect the industry norm. The option period shall begin with disclosure of the Intellectual Property to the Company and shall terminate 6 months thereafter. In any event, the University shall have the right to use Intellectual Property for research, teaching and administrative purposes.

* **What does it cover?**

## Intellectual Property: The University shall own all intellectual property, including technical information, know-how, copyrights, models, drawings, specifications, prototypes, inventions and software developed by University personnel in performance of the Project (“Intellectual Property”). The Company shall have the first option on an exclusive or non-exclusive licence to commercially exploit the Intellectual Property on terms (including compensation to the University) that generally reflect the industry norm. The option period shall begin with disclosure of the Intellectual Property to the Company and shall terminate 6 months thereafter. In any event, the University shall have the right to use Intellectual Property for research, teaching and administrative purposes.

* **Who Owns It?**

## Intellectual Property: The University shall own all intellectual property, including technical information, know-how, copyrights, models, drawings, specifications, prototypes, inventions and software developed by University personnel in performance of the Project (“Intellectual Property”). The Company shall have the first option on an exclusive or non-exclusive licence to commercially exploit the Intellectual Property on terms (including compensation to the University) that generally reflect the industry norm. The option period shall begin with disclosure of the Intellectual Property to the Company and shall terminate 6 months thereafter. In any event, the University shall have the right to use Intellectual Property for research, teaching and administrative purposes.

* **Grant of Rights**

## Intellectual Property: The University shall own all intellectual property, including technical information, know-how, copyrights, models, drawings, specifications, prototypes, inventions and software developed by University personnel in performance of the Project (“Intellectual Property”). The Company shall have the first option on an exclusive or non-exclusive licence to commercially exploit the Intellectual Property on terms (including compensation to the University) that generally reflect the industry norm. The option period shall begin with disclosure of the Intellectual Property to the Company and shall terminate 6 months thereafter. In any event, the University shall have the right to use Intellectual Property for research, teaching and administrative purposes.

* **Retained Rights**

## Intellectual Property: The University shall own all intellectual property, including technical information, know-how, copyrights, models, drawings, specifications, prototypes, inventions and software developed by University personnel in performance of the Project (“Intellectual Property”). The Company shall have the first option on an exclusive or non-exclusive licence to commercially exploit the Intellectual Property on terms (including compensation to the University) that generally reflect the industry norm. The option period shall begin with disclosure of the Intellectual Property to the Company and shall terminate 6 months thereafter. In any event, the University shall have the right to use Intellectual Property for research, teaching and administrative purposes.

## All inventions, discoveries, new uses, improvements, processes and/or compounds that may arise in the course of the Clinical Trial (“Intellectual Property”) and all information and results produced, generated or developed by the INVESTIGATOR and/or INSTITUTION in the course of the Clinical Trial (“Data”) shall be owned by the SPONSOR. The SPONSOR hereby grants to the INSTITUTION and the INVESTIGATOR a non-exclusive, royalty-free license to use all Intellectual Property and Data for their own academic and research purposes and for publication in accordance with Article 7.0 herein. The SPONSOR hereby grants to the INSTITUTION and the INVESTIGATOR the right to provide all clinical information relating to a specific Subject to that Subject (or his or her lawful representative). The INVESTIGATOR shall be entitled to retain a copy of all Data and to obtain from SPONSOR a summary of the analysed data generated by other sites participating in the multi-centre Clinical Trial.

## All inventions, discoveries, new uses, improvements, processes and/or compounds that may arise in the course of the Clinical Trial (“Intellectual Property”) and all information and results produced, generated or developed by the INVESTIGATOR and/or INSTITUTION in the course of the Clinical Trial (“Data”) shall be owned by the SPONSOR. The SPONSOR hereby grants to the INSTITUTION and the INVESTIGATOR a non-exclusive, royalty-free license to use all Intellectual Property and Data for their own academic and research purposes and for publication in accordance with Article 7.0 herein. The SPONSOR hereby grants to the INSTITUTION and the INVESTIGATOR the right to provide all clinical information relating to a specific Subject to that Subject (or his or her lawful representative). The INVESTIGATOR shall be entitled to retain a copy of all Data.

* **What does it cover?**

## Definition of IP should only include things created in the course of the project (i.e. not pre-existing IP or IP created after the fact)

## Can distinguish between patentable/not patentable IP

## Should be inclusive not exclusive list (i.e. defined as “including ….”

## Be careful of including “ideas, thoughts, concepts” if you don’t own IP

* **Background IP**

## (a) “Background Intellectual Property" means Intellectual Property of a Party that is:

## (i) Proprietary to that Party and was conceived, created, or developed prior to, or independent of, any research performed pursuant to this Agreement; and

## (ii) Necessary for the performance of the Project.

## (b) "Foreground Intellectual Property" means any Intellectual Property that is conceived, created, or developed by a Party in the course of performing the Project.

## (c) “Intellectual Property” means all intellectual property, including without limitation technical information, know-how, copyrights, patents and trade secrets, ideas, thoughts, concepts, processes, techniques, data, development tools, models, drawings, specifications, prototypes, inventions and software, that is discovered, created or reduced to practice in performance of the Project.

Lecture 28  
Intellectual Property (Cont’d)

**28.1 Who Owns It?**

## Depends on the circumstances of the Project, nature of funding and the policies of the institution

## Grant – Institution should own

## Collaboration – Each should own IP it creates

## Service contract – Sponsor should own

## Regardless of inventor/institution policy, in the IP clause it is better to have ownership vest in Institution in the first instance

## If you are giving up ownership of IP in agreement make sure you own it in the first place.

* **I am paying for it so I should own it...**

## In a collaborative research project a sponsor is never paying the full cost of the research. Overhead alone do not account for the resources that the institution is bringing to the project (including the PI’s expertise and often matching funding). In a collaborative project the parties are working together and thus should both benefit from the results.

* **Ownership in a Collaborative Project**

## Company shall own all Foreground Intellectual Property conceived entirely by Company personnel (“Company IP"). University shall own all Foreground Intellectual Property conceived entirely by University personnel ("University IP"). The Parties shall jointly own any Foreground Intellectual Property conceived of by at least one individual employed by Company and at least one individual within the University (“Joint IP”).

## Each Party agrees to disclose promptly to the other Parties any and all Foreground Intellectual Property created by or on behalf of that Party under the Project to the other Parties regardless of whether or not capable of protection by patents, copyrights, industrial designs or design patents.

* **Grant of Rights**

## What rights of use that are given to the sponsor (or institution) again depends on the nature of the project, the type of funding and the policies of the institution

## A license is the right of the party to use the IP. Can be limited by field, duration, geographical area, or exclusivity

## An exclusive right means that the only person that can use the IP is the licensee – even to the exclusion of the owner

## Grant of rights should be given as a time limited option. The length of time depends on the nature of the IP & industry.

## Try to avoid setting royalty rates in the research agreement

## Once Sponsor turns down option you should have freedom to deal with IP as you see fit.

* **Retained Rights**

## If you do not own the IP or are granting an exclusive right to use the IP to someone then you need to retain the right to use the IP for your researcher.

## This would include the right to use the IP for research, teaching, publication purposes

## Be aware of how giving up ownership of IP affects the rest of the agreement, particularly the publication clause and confidentially clause

* **Right to assign IP to Inventors**

## The University may assign all right, title and interest which the University may in the future have in University IP and Joint IP to the University inventors according to the University’s Inventions Policy and to the terms and conditions of this Agreement.

* **Indemnity/Liability**

## Important not to be responsible for use of the IP by the sponsor

## Indemnity:vThe Company shall indemnify and save harmless the University ..... Against all ... claims ... resulting from the use by the Company or its affiliates, its customers or licensees of any deliverable or intellectual property developed by the University or the Company under this Agreement.

* **Limitation of Liability**

## The INSTITUTION shall not be liable for any direct, indirect, consequential, or other damages suffered by the SPONSOR or any third party resulting from the use of the Data or Intellectual Property developed under this Agreement, Protocol and Clinical Trial, except to the extent such damages arise from the negligence or wilful misconduct of the INSTITUTION. The entire risk as to the use of the Data and Intellectual Property and the design, development, manufacture, offering for sale, sale or other disposition and performance of all products incorporating same, including but not limited to the Study Drug, is assumed by the SPONSOR.

* **Duration of protection**

## Life + 50

## 50

## 20

## 15

## 10

## Payment of statutory fee

* **Ownership**

## Who is the owner?

## Proper plaintiff rule

## Employer and employee relationship

## Independent contractor

## Government employee

## Joint-ownership

## Commissioned works

* **Exclusive rights**

## To control the whole or a substantial part of the work.:-

## The reproduction in any material form

## The communication to the public

## The public performance, showing or playing

## Distribution by sale or other transfer

## Commercial rental to the public

* **The exception to the exclusive right**

## Fair dealing exception

## Statutory exception under section 13(2)

## Temporal (duration)

## Geographic

## Non-material works

## Compulsory licenses

* **Enforcing IP rights**

## Civil action

## Criminal prosecution

## Cost in litigation

## Assistance from Enforcement Division

## Being vigilant/ self help

* **Civil action**

## Starting a civil action

## Advantages

## Liability for cost

## Monetary compensation in term of damages

* **Criminal prosecution**

## Making a complaint

## Police or enforcement division

## Cost borne by the government

## No monetary compensation

## Remedy in term of fines or imprisonment for the offender

* **IP infringement**

## Primary infringement

## Who does or causes

## Making the product

## Secondary infringement

## Commercial activities

## Selling, distribution for sale etc

* **Secondary infringement**

## sells,lets for hire or by way of trade exposes or offer for sale or hire any infringing copies.

## Distribute infringing copies.

## Importing into the country

* **Commercialization**

## Assignment

## Licenses

## - Exclusive

## - Non-exclusive

Lecture 29  
Information Security

**29.1 Overview**

## The CIA

## Security Governance

### Policies, Procedures, etc.

### Organizational Structures

### Roles and Responsibilities

## Information Classification

## Risk Management

* **The CIA: Information Security Principles**

## Confidentiality

### Allowing only authorized subjects access to information

## Integrity

### Allowing only authorized subjects to modify information

## Availability

### Ensuring that information and resources are accessible when needed

* **Reverse CIA**

## Confidentiality

### Preventing unauthorized subjects from accessing information

## Integrity

### Preventing unauthorized subjects from modifying information

## Availability

## Preventing information and resources from being inaccessible when needed

* **Using the CIA**

## Think in terms of the core information security principles

## How does this threat impact the CIA?

## What controls can be used to reduce the risk to CIA?

## If we increase confidentiality, will we decrease availability?

* **Security Governance**

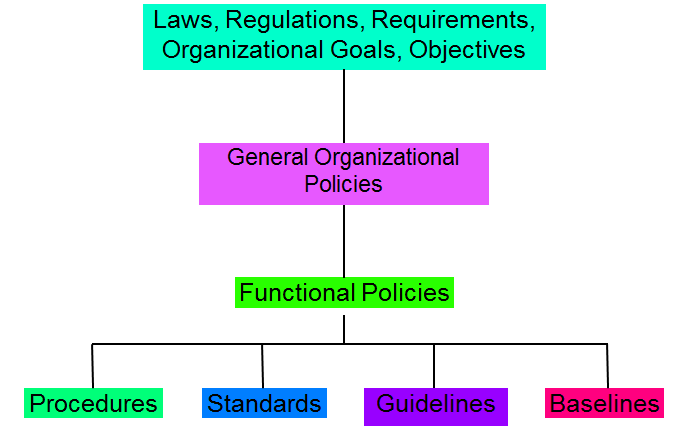
## Security Governance is the organizational processes and relationships for managing risk

### Policies, Procedures, Standards, Guidelines, Baselines

### Organizational Structures

### Roles and Responsibilities

* **Policy Mapping**

****

**Figure 29.1: Policy Mapping**

* **Policies**

### Policies are statements of management intentions and goals

### Senior Management support and approval is vital to success

### General, high-level objectives

### Acceptable use, internet access, logging, information security, etc

* **Procedures**

### Procedures are detailed steps to perform a specific task

### Usually required by policy

### Decommissioning resources, adding user accounts, deleting user accounts, change management, etc

* **Standards**

### Standards specify the use of specific technologies in a uniform manner

### Requires uniformity throughout the organization

### Operating systems, applications, server tools, router configurations, etc

* **Guidelines**

### Guidelines are recommended methods for performing a task

### Recommended, but not required

### Malware cleanup, spyware removal, data conversion, sanitization, etc

* **Baselines**

### Baselines are similar to standards but account for differences in technologies and versions from different vendors

### Operating system security baselines

### FreeBSD 6.2, Mac OS X Panther, Solaris 10, Red Hat Enterprise Linux 5, Windows 2000, Windows XP, Windows Vista, etc

Lecture 30  
Information Security (Cont’d)

**30.1 Overview**

## Organizational Structures Roles and Responsibilities

## Information Classification

## Risk Management

* **Organizational Structure**

## Organization of and official responsibilities for security vary

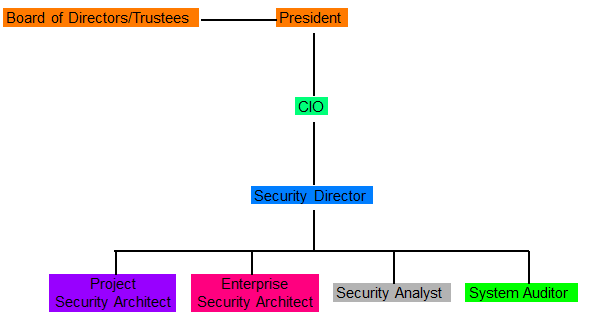
### BoD, CEO, BoD Committee

### Director, Manager

## IT/IS Security

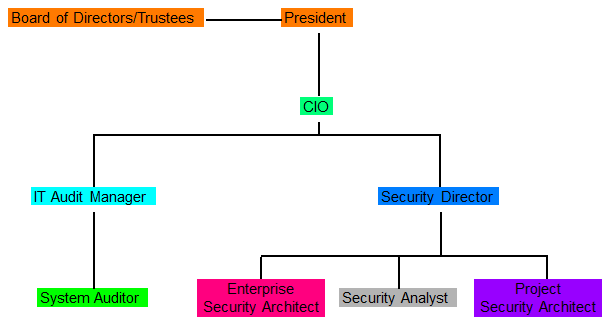
## Audit

* **Typical Organizational Chart**

****

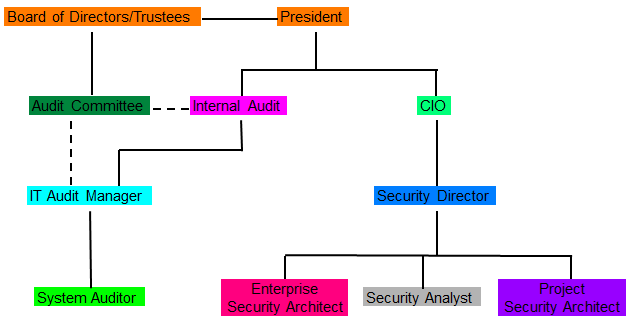
**Figure 30.1: Typical Organizational Chart**

* **Security-Oriented Org Chart**

****

**Figure 30.2: Security-Oriented Org Chart**

* **Further Separation**

****

**Figure 30.3: Further Separation**

* **Organizational Structure**

## Audit should be separate from implementation and operations

### Independence is not compromised

## Responsibilities for security should be defined in job descriptions

## Senior management has ultimate responsibility for security

## Security officers/managers have functional responsibility

* **Roles and Responsibilities**

## Best Practices:

### Least Privilege

### Mandatory Vacations

### Job Rotation

### Separation of Duties

## Owners

### Determine security requirements

## Custodians

### Manage security based on requirements

## Users

### Access as allowed by security requirements

* **Information Classification**

### Not all information has the same value

### Need to evaluate value based on CIA

### Value determines protection level

### Protection levels determine procedures

### Labeling informs users on handling

## Government classifications:

### Top Secret

### Secret

### Confidential

### Sensitive but Unclassified

## Private Sector classifications:

### Confidential

### Private

### Sensitive

### Public

## Criteria:

### Value

### Age

### Useful Life

### Personal Association

* **Risk Management**

## Risk Management is identifying, evaluating, and mitigating risk to an organization

### It’s a cyclical, continuous process

### Need to know what you have

### Need to know what threats are likely

### Need to know how and how well it is protected

### Need to know where the gaps are

* **Identification**

## Assets

## Threats

### Threat-sources: man-made, natural

## Vulnerabilities

### Weakness

## Controls

### Safeguard

Lecture 31 & 32  
Risk Management

**32.1 Threat Identification**

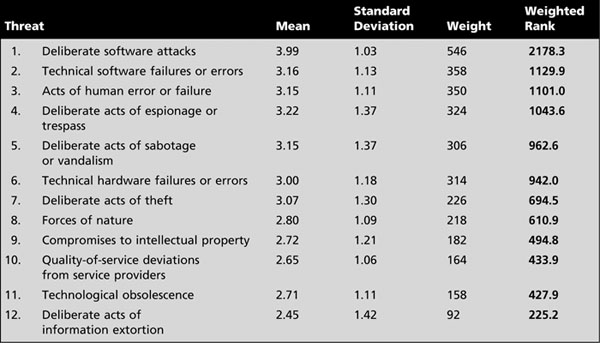
* **Vulnerability Assessment**

Begin to review every information asset for each threat

This review leads to the creation of a list of vulnerabilities that remain potential risks to the organization

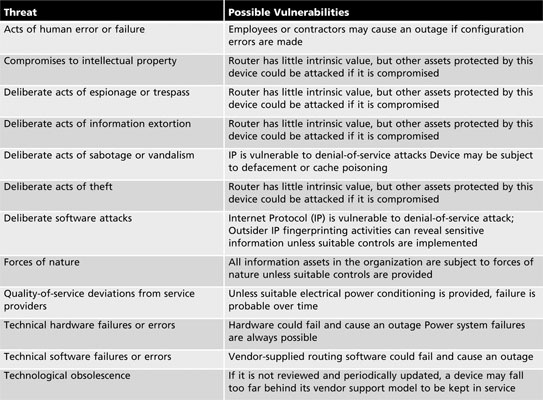
* Vulnerabilities are specific avenues that threat agents can exploit to attack an information asset

At the end of the risk identification process, a list of assets and their vulnerabilities has been developed



**Figure 32.1 Threat Identification**

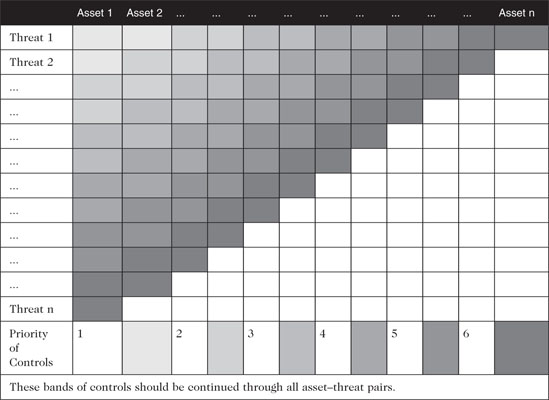
This list serves as the starting point for the next step in the risk management process - risk assessment



**Figure 32.2 Threat Identification**

**32.2 The TVA Worksheet**

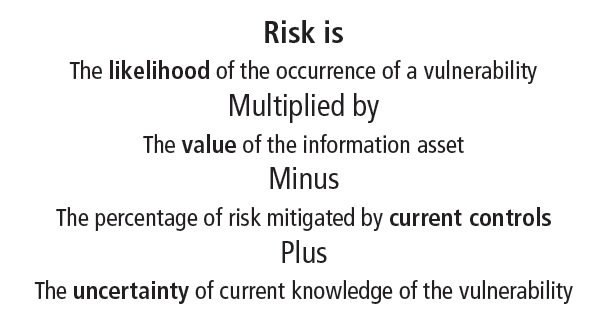
At the end of the risk identification process, a list of assets and their vulnerabilities has been developed. Another list prioritizes threats facing the organization based on the weighted table discussed earlier. These lists can be combined into a single worksheet.



**Figure 32.3: The TVA Worksheet**

* **Introduction to Risk Assessment**

The goal is to create a method to evaluate the relative risk of each listed vulnerability



**Figure 32.4: Introduction to Risk Assessment**

* **Likelihood**

The overall rating of the probability that a specific vulnerability will be exploited

* Often using numerical value on a defined scale (such as 0.1 – 1.0)

Using the information documented during the risk identification process, you can assign weighted scores based on the value of each information asset, i.e. 1-100, low-med-high, etc

* **Assessing Potential Loss**

Questions to ask when assessing potential loss

* Which threats present a danger to this organization’s assets in the given environment?
* Which threats represent the most danger to the organization’s information?
* How much would it cost to recover from a successful attack?

Questions to ask when assessing potential loss (cont’d.)

* Which threats would require the greatest expenditure to prevent?
* Which of the aforementioned questions is the most important to the protection of information from threats within this organization?
* **Percentage of Risk Mitigated by Current Controls**

If vulnerability is fully managed by an existing control, it can be set aside. If it is partially controlled, estimate what percentage of the vulnerability has been controlled.

**Uncertainty**

It is not possible to know everything about each vulnerability. The degree to which a current control can reduce risk is also subject to estimation error. Uncertainty is an estimate made by the manager using judgment and experience.

**Risk Determination**

**Example**

Asset A has a value of 50 and has one vulnerability, which has a likelihood of 1.0 with no current controls. Your assumptions and data are 90% accurate

Asset B has a value of 100 and has two vulnerabilities: vulnerability #2 has a likelihood of 0.5 with a current control that addresses 50% of its risk; vulnerability # 3 has a likelihood of 0.1 with no current controls. Your assumptions and data are 80% accurate

The resulting ranked list of risk ratings for the three vulnerabilities is as follows:

* Asset A: Vulnerability 1 rated as 55 = (50 × 1.0) – 0% + 10%
* Asset B: Vulnerability 2 rated as 35 = (100 × 0.5) – 50% + 20%
* Asset B: Vulnerability 3 rated as 12 = (100 × 0.1) – 0 % + 20%

**Likelihood and Consequences**   
Likelihood and consequence rating

* Another approach
* From the Australian and New Zealand Risk Management Standard 4360i
* Uses qualitative methods of determining risk based on a threat’s probability of occurrence and expected results of a successful attack
* Consequences (or impact assessment) are evaluated on 5 levels ranging from insignificant (level 1) to catastrophic (level 5), as assessed by the organization
* Qualitative likelihood assessments levels are represented by values ranging from A (almost certain) to E (rare), as determined by the organization

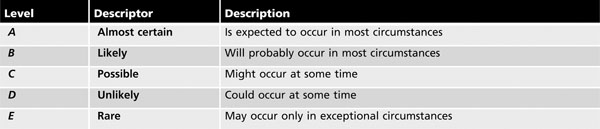
**Identify Possible Controls**

For each threat and its associated vulnerabilities that have residual risk, create a preliminary list of control ideas. Three general categories of controls exist:

* Policies
* Programs
* Technical controls



**Figure 32.5: Likelihood and Consequences 1**

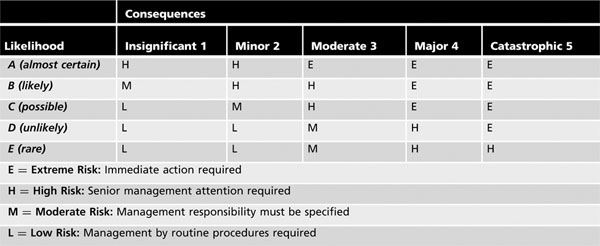


**Figure 32.6: Likelihood and Consequences 2**

Consequences and likelihoods are combined

* Enabling the organization to determine which threats represent the greatest danger to the organization’s information assets

The resulting rankings can then be inserted into the TVA tables for use in risk assessment



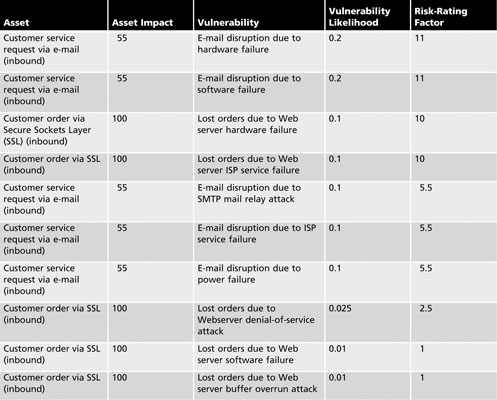
**Figure 32.7: Likelihood and Consequences 3**

**Documenting the Results of Risk Assessment**

Goals of the risk management process

* To identify information assets and their vulnerabilities
* To rank them according to the need for protection

In preparing this list, a wealth of factual information about the assets and the threats they face is collected. Information about the controls that are already in place is also collected. The final summarized document is the ranked vulnerability risk worksheet.

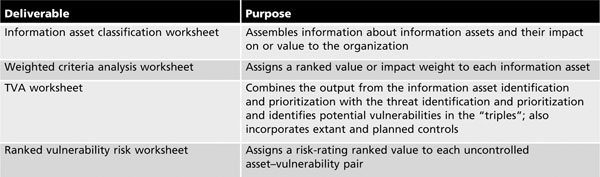


**Figure 32.8: Documenting the Results of Risk Assessment 1**

What should the documentation package look like?

What are the deliverables from this stage of the risk management project?

The risk identification process should designate what function the reports serve, who is responsible for preparing them, and who reviews them.



**Figure 32.9: Documenting the Results of Risk Assessment 2**