Information Systems Security

Arrianto Mukti Wibowo, M.Sc.,
Faculty of Computer Science
University of Indonesia
amwibowo@cs.ui.ac.id

Laws, Investigations & Ethics

Tujuan

- Mempelajari berbagai jenis aturan yang terkait dengan kejahatan komputer dan legalitas transaksi elektronik, serta membahas masalah etika dalam dunia komputer.

Topik

- Laws and ethics on computer crime, electronic transactions, piracy, intellectual property, computer crime investigations, security import & export laws, privacy issues.

Ethical & Social Impact of Information Systems

Objective

- To provide a basic understanding of ethical & social problems in the information society
- To provide background issues for further discussions on later weeks

Discussion Topics

- Opening topic: the Internet
- Understanding ethics
- Ethics in information society
- Moral dimensions of information systems
  - Information rights
  - Intellectual property
  - Accountability, Liability & Control
  - System Quality
  - Quality of Life

The Internet

- The Internet
- Tell me both pros & cons of the Internet!
- How about cell phones & SMS?

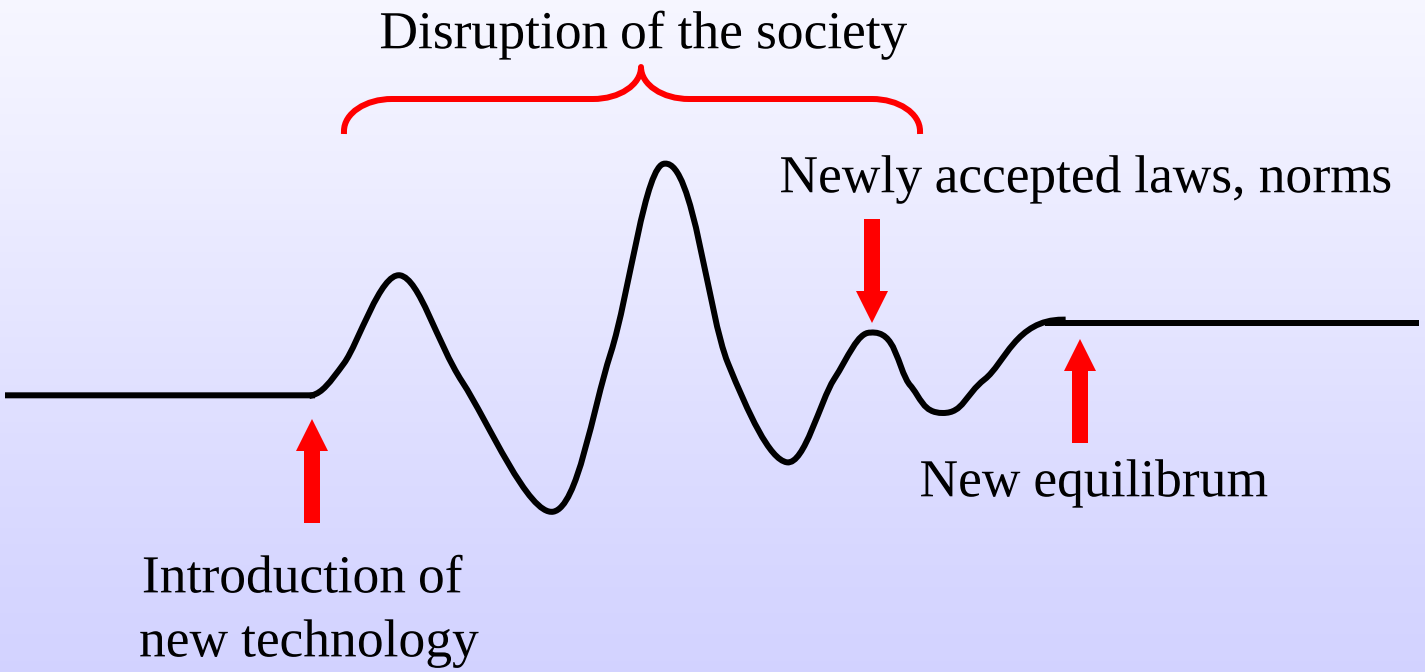
So?

Technology is a double edged sword

Ethics

- Principles of right & wrong that can be used by individuals acting as a moral agents to make choices to guide their behaviour
- IT can be used to achieve social progress (e.g. economic development, healthier environment, better understanding among cultures)
- But IT can also be used to commit crimes!

Equilibrum of the Society



Technology Trends

Trend	Impact
Moore's Law: Computing power doubles every 18 months	More organization depend on computers for critical operations
Rapidly declining data storage costs	Organizations can easily maintain detailed database on individuals
Datamining advances	Companies can analyze vast quantities of data gathered on individuals to develop detailed profiles of individuals behaviour
Ease of networking	Copying data from one location to another and accessing data from remote locations will be easier

Do you think this is a problem?

Profiling...

- The use of computers to combine data from multiple sources and create electronic dossier of detailed information on individuals
- What technologies can be used to create information of an individual behaviour?
  - credit & debit cards
  - Internet proxies
  - cookies

Ethics in an Information Society

Basic concepts

- Responsibility
  - accepting the potential cost, duties, & obligations for the decisions one makes
- Accountability
  - the mechanism to determine who took responsible action, and who is responsible (who took what action)

- Liability
  - the existance of laws that permit individuals to recover the damages done to them by other person

Ethical Analysis of Information Systems

- Computers do not act by themselves. "Impacts" are products of individual or organizational actions / behaviour.
- Responsibility for the consequence of technology falls to the user of the technology
- "Victims" can recover damages done to them

Ethical Analysis Methodology

- Identify & describe clearly the facts
- Define the confilct dilema and identify the higher order values involved
- Identify the stakeholders
- Identify the options that you can take reasonably
- Identify the potential consequence of your opinion

Candidate Ethical Principles

- **Golden Rule**. Do to the others as you would do to them. (Do not do to the others) as you (do not want others) to do to you
- **Kant's Categorical Imperative**. If an action is not right for everyone to take, then it is not right for everyone
- **Descartes' rule of change**. If an action can not be taken repeated, then it is not right to be taken in any time

- **Utilitarian principle.** One could put values in rank order an understand the consequence of various courses of action.
- **Risk Aversion principle.** Action taken should produce the least harm or incures the least cost.
- **No "Free Lunch" principle**. Assume that all objects (tangible & intangible) are owned by someone unless there is a specific declaration. Assume the creator wants compensation for this work.

Professional Code of Conduct

- Promulgated by professional associations
  - Doctors
  - Association of Computing Machinery
  - Certified IS Auditors

Some Cases

- Downsizing with technology: employee layoffs
- Electronic profiling at the airport
- Employee monitoring on the Internet
- What do you think?

Moral Dimensions of Computers

Privacy

Information Rights

- Privacy:
  - claim of individuals to be left alone, free from surveillance or interference from other individuals, organization or state
- Why do some culture value privacy more than the others?
- Historical background:
  - freedom of religious interpretation
  - America: land of freedom
  - “it is none of your business”

Fair Information Practice

- Written in 1973 by federal committee
- Based on “mutual interest” between record holder & the individual

FIP Principles

- No personal record systems is secret
- Individuals have the right to access, inspect, review, and amendment to systems that contain information about them
- There must be no use of personal information other than those for which it was gathered without prior consent

Cont'd

- Managers of information systems are responsible and can be held accountable & liable for the damage done by systems
- Governments have the right to intervene in the information relationships among private parties

Internet Challenges to Privacy

- Record on-line activities: Amazon.com
- Cookies

Spamming

- The practice of sending unsolicited e-mail and other electronic communication
- Options:
  - unsubscribe
  - filter
- Used by marketing companies, the collect e-mails from the Internet:
  - mailing list
  - web pages

Issues

- Do we have to inform customers that we are monitoring their behaviour?
- Are we allowed to use health records to screen insurance applicants?
- What do we consider private territory?
- What about secure transmissions & wiretapping? SSL 1028 bit?

Intellectual Property

Property Rights: Intellectual Propoerty

- Intangible property created by individuals or corporations that is subject to protections under trade secret, copyright & patent law.
- For instance:
  - Trade Secrets
  - Copyright
  - Patent

Trade Secrets

- Any intellectual work or product used for a business purpose that can be classified as belonging to that business, provided it is not based on information in the public domain
- Protects the main ide, the “engine”, the “how it works” of the software
- Requires employees’ non disclosure agreement
- When the software is widely used and dissassembled, the “engine” could be known by public

Copyright

- Statutory grant that protects creators of intellectual property against copying by others for any purpose for a certain period.
- Books, lectures, dramas, musical composition, computer software
- Intention of copyright laws: creative people receive financial & other benefits from their work.

- Benefit: protection against illegal copying
- Drawbacks: the idea is not protected, only its manifestation

Patents

- A legal document that grants the owner an exclusive monopoly on the ideas behind an invention for several years
- Designed to ensure that inventors of new machines or methods are rewarded for their labor while making wirespread use of their inventions

- Requires originality, novelty & invention
- Strength: monopoly of the underlying ide, while the ide is known to the public
- However, the ide must pass stringent criteria at the Patent Office

Challenges to Intellectual Property Rights

- Digital media: ease of copying (theft)
- Case: Sim Lim at Singapore
- Allowing citiezens to keep up with technology?
- Case: MP3, Napster, Gnutella (source code)
- Web framing

Accountability, Liability & Control

Some Problems

- ATMs of a bank is out of order for one day
- Customers can not withdraw any money
- Who is liable for the loss?
  - The bank
  - The ATM vendor

Managing Risk

- The use of risk management is important
- Service providers must have disaster recovery plan (DRP).
- Also called “Business Continuity Plan” (BCP)
- BCP includes legal matters and customer response guidelines during disaster

Case: Network Service Provider

- Would ISP be liable for:
  - spamming?
  - Trojan horse & internet virus?
  - Pornography?

System Quality:
Data Quality & System Errors

The Impossible: Zero Defect

- Impossible to create "zero defect" softwares
- The importance of testing (remember debugging & testing in Java?)
- Formal methods: can significantly decrease defects (still can not achieve 0% defect)
- Perfect software >> never be released >> no sales >> no money!

Data Quality

- System should ensure data in the computers are accurate
- Some “computer errors” are actually made by human

Standards

- Should there be IT Management standards?
- Example:
  - Control Objectives for IT Governance
  - ISO 17799 IT Management Security
  - Software Quality Assurance

Quality of Life

Rapidity of Change

- Information technology creates a very efficient market
- Information pours like water
- Company must adjust fast to competition, based on the information
- What are the impact to the employees:
  - stress
  - just in time workplace

Nomadic Computing

- The danger of obiquitous computing & telecommunication
- Where is the family & work boundaries?
- Pros:
  - supports the idea of “knowledge workers”
  - be close to family
  - saves energy, less polution
- Cons:
  - no private time
  - home but “not at home”

Digital Divide

- The right for information access
- Is it a already a real problem in Indonesia?
- What do you think you can achieve by narrowing the digital divide?

Technostress

- Induced by computer used
- Human expects fast response, because of their interaction with computers
- Will get impatient when confronted with slow response system, or with other "slow reacting" human / institutions!

Computer Crime

Agenda

- Case & Example
- Definition
- Computer Crime Modus

Computer Crime Definitions

- Encyclopedia of Crime & Justice, *"any illegal act requiring knowledge of computer technology for its perpetration, investigation or prosecution"*

Classic Case: BNI 1987

- Fund transfer of US$ 9 million from BNI New York to foreign bank accounts
- Used remote access from a hotel, with stolen password
- Was a new case at that time for Indonesia!

Recent Case

- Wendy Setiawan (15) hacked Data Storage Institute website, Singapore, from an Internet Café in Singapore
- Liable on conviction to a fine $5000, 3 years in prison (max)

Definitions

- Encyclopedia of Crime & Justice, *"any illegal act requiring knowledge of computer technology for its perpetration, investigation or prosecution"*

Forms of Computer Crime

- According to Stair (1986)
  - deletion, addition & modification part of whole data in a computer system
  - modify / develop programs for criminal purpose
  - use computer for criminal purpose

Computer Crime Modus

- Data diddling: modifying data as they being entered into computer (low-tech!)
- Trojan horse
- Salami technique / rounding down
- Viruses (inserted to other programs)
- Worms (do not change other program)
- Data leakage: stealing computer generated reports...

Modus (2)

- Piggybacking: following a person, or an acceptable/valid data packet
- Impersonation: being someone else, in the real world or electronically
  - spoofing: IP, e-mail
- Denial of service
- Computer shut down
- Wire-tapping: eavesdropping over telecommunication line

Modus (3)

- Logic bombs, by disgruntled employees
- War dialing: finding a modem pool from a telephone book
- Spamming
- E-mail flaming
- Scavenging, from deleted(!) files

Targets

- Competitors
- Financial institutions
- Government & military agencies
- Enemy
- Well know portals / websites
- Anything (for fun)

Impacts

- Financial loss: direct or indirect
- Legal repercussions: breach of law (by being ignorant of security)
- Loss of credibility: case of kilkbca.com
- Blackmail: threatening someone
- Industrial espionage
- Disclosure of information
- Sabotage

Violators

- Hackers
- Employees
- IS personnel
- End users
- Former employees
- Interested or educated outsiders
- Part-time & temporary staffs
- Vendors & consultants
- Accidental ignorant

Controling Crimes

- Preventive: do not allow access for guest into data centre
- Detective: always use anti virus programs
- Curative: system backups

Publish or Not to Publish

- Reasons to keep vulnerabilities secret
  - to enhance security
- Reasons to dislose vulnerabilities
  - to enhance security…!
  - Why?
  - Eventually the bad guys will know the vulnerabilities. It is better the good guys to know the vulberabilities first!

Attack or Defend?

- If a hacker is known to enter a computer system, there are two options to consider:
  1. Protect & proceed
  2. Pursue & prosecute

Reasons for Protect & Proceed

a. the computer system was not actually protected before

b. if not protected, financial loss will be staggering

c. cost for prosecution is expensive

d. legitimate users in the network would face considerable threat.

e. if the business is vulberable to lawsuits from the users or customers.

f. the legal infrastructure is still weak

Reasons for Pursue & Prosecute

a. the network & computer system had already been well protected

b. the system had already been struck several times before

c. the attack is/was concentrated

d. the computer system is highly popular / visible

e. while tracking the attacker, don't mind the attacker use a few computer resource (as long as considered not yet dangerous)

f. attacker's access can be limited

g. tools to monitor the attacker are sufficient

h. the network administrator is sufficiently clever

i. the managers are willing to press charges

j. know what kind of evidence would lead to prosecution

k. a system & data backup exist

l. a working law exist, including knowledgeable law enforcement

m. if not punished, the attacker will re-attack

Personnel Security

- Human is the most vulnerable part in computer security
- Screening employees
- Segregation of jobs of IS personnel
- Job rotation
- Termination of access rights of after termination
- Employee awareness program

New Topics

- Password sharing?
- Cybersquatters
- Framing
- Typosquatters

Computer Forensics

Definisi

- **"Identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings** (i.e., a court of law)," according to D. Rodney McKemmish (Computer and Intrusion Forensics)
- An IS auditor may be required or asked to be involved in a forensic analysis in progress to provide expert opinion or to ensure the correct interpretation of information gathered.
- It is very important to maintain evidence in any situation. Most organizations are not well equipped to deal with intrusions and electronic crimes from an operational and procedural perspective and they respond to it only when the intrusion has occurred and the risk is realized.
- The evidence loses its integrity when the decision chain is inappropriately managed and the intrusion is responded to in an ad hoc manner.

Alat Bukti Elektronik

- For evidence to be admissible in a court of law, the chain of custody needs to be maintained professionally. The chain of evidence essentially contains information regarding:
  - Who has had access to the evidence (chronological manner)?
  - What procedures did they follow in working with the evidence (disk duplication, virtual memory dump)?
  - How can it be shown that the analysis is based on copies that are identical to the original evidence (could be documentation, checksums, timestamps)?

Tahapan Forensik Komputer

- There are four major consideration and chain of events in regards to evidence in computer forensics:
  - Identify—Refers to the identification of the type of information that is available and the best means to retrieve it
  - Preserve—Refers to the practice of preserving evidence with the least amount of changes possible
  - Analyze—It involves, extracting, processing and interpreting the evidence. Extracted data could be nonunderstandable binary data, after it is processed and converted into human readable format. Then, interpreting requires in-depth knowledge of how things fit together.
  - Present—Presentation would be to various audiences, such as management, attorneys, court, etc. Acceptance of the evidence depends upon the manner of presentation (as it should be convincing), qualifications of the presenter, and credibility of the process used to preserve and analyze the evidence.

Indonesian Laws

- UU no.39/1999 Telekomunikasi
- RUU Informasi & Transaksi Elektronik