HUM 4441
ENGINEERING ETHICS

Dr. Mohammad Rezwanul Huq

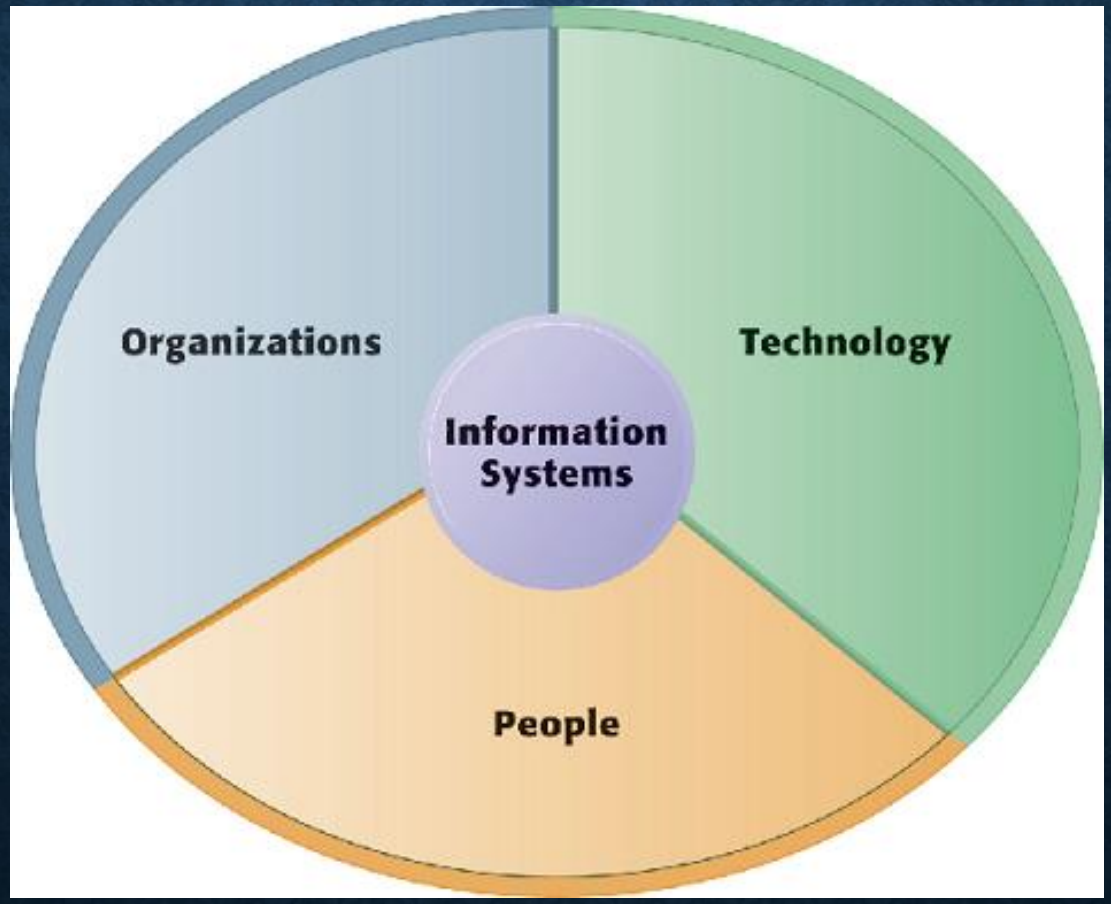
Adjunct Faculty, IUT

ETHICAL AND SECURITY ISSUES IN INFORMATION SYSTEMS

INFORMATION SYSTEMS

- “Information systems (IS) is the study of complementary networks of hardware and software that people and organizations use to collect, filter, process, create, and distribute data.” [Wikipedia]
- “Information systems are combinations of hardware, software, and telecommunications networks that people build and use to collect, create, and distribute useful data, typically in organizational settings.” [Information Systems Today - Managing in the Digital World, fourth edition. Prentice-Hall, 2010]
- “Information systems are interrelated components working together to collect, process, store, and disseminate information to support decision making, coordination, control, analysis, and visualization in an organization.” [Management Information Systems, twelfth edition, Prentice-Hall, 2012.]

DIMENSIONS OF IS



TECHNOLOGICAL COMPONENTS OF IS

- Hardware
- Software
- Data
- Networking Communication

PEOPLE

- From the front-line help-desk workers, to systems analysts, to programmers, all the way up to the chief information officer (CIO), the people involved with information systems are an essential element.

ORGANIZATIONS

- The last component of information systems is the organization and it's processes.
- An organizational process is a series of steps undertaken to achieve a desired outcome or goal.
- Information systems are becoming more and more integrated with organizational processes, bringing more productivity and better control to those processes.

EVOLUTION OF IS

Era	Hardware	Operating System	Applications
Mainframe (1970s)	Terminals connected to mainframe computer.	Time-sharing (TSO) on MVS	Custom-written MRP software
PC (mid-1980s)	IBM PC or compatible. Sometimes connected to mainframe computer via expansion card.	MS-DOS	WordPerfect, Lotus 1-2-3
Client-Server (late 80s to early 90s)	IBM PC "clone" on a Novell Network.	Windows for Workgroups	Microsoft Word, Microsoft Excel
World Wide Web (mid-90s to early 2000s)	IBM PC "clone" connected to company intranet.	Windows XP	Microsoft Office, Internet Explorer
Web 2.0 (mid-2000s to present)	Laptop connected to company Wi-Fi.	Windows 7	Microsoft Office, Firefox
Post-PC (today and beyond)	Apple iPad	iOS	Mobile-friendly websites, mobile apps

RISKS WITH IS

- Information systems have made many businesses successful today. Some companies such as Google, Facebook, eBay, etc. would not exist without information technology.
- However, improper use of information technology can create problems for the organization and employees.

CYBER CRIME

- Cyber-crime refers to the use of information technology to commit crimes.
- Cyber-crimes can range from simply annoying computer users to huge financial losses and even the loss of human life.
- The growth of smartphones and other high-end Mobile devices that have access to the internet have also contributed to the growth of cyber-crime.

IDENTIFY THEFT

- Identity theft occurs when a cyber-criminal impersonates someone else identity to practice malfunction. This is usually done by accessing personal details of someone else.
- One of the ways that cyber-criminals use to obtain such personal details is **phishing**.
- **Phishing** involves creating fake websites that look like legitimate business websites or emails.

COPYRIGHT INFRINGEMENT

- **Piracy** is one of the biggest problems with digital products. Websites such as the pirate bay are used to distribute copyrighted materials such as audio, video, software, etc.
- Copyright infringement refers to the unauthorized use of copyrighted materials.

CLICK FRAUD

- Advertising companies such as Google AdSense offer pay per click advertising services.
- **Click fraud** occurs when a person clicks such a link with no intention of knowing more about the click but to make more money. This can also be accomplished by using automated software that makes the clicks.

ADVANCE FEE FRAUD

- An email is sent to the target victim that promises them a lot of money in favor of helping them to claim their inheritance money.
- If the victim sends the money to the scammer, the scammer vanishes and the victim loses the money.

HACKING

- **Hacking** is used to by-pass security controls to gain unauthorized access to a system.
  - Install programs that allow the attackers to spy on the user or control their system remotely
  - Deface websites
  - Steal sensitive information. This can be done using techniques such as SQL Injection, exploiting vulnerabilities in the database software to gain access, social engineering techniques that trick users into submitting ids and passwords, etc.

COMPUTER VIRUS

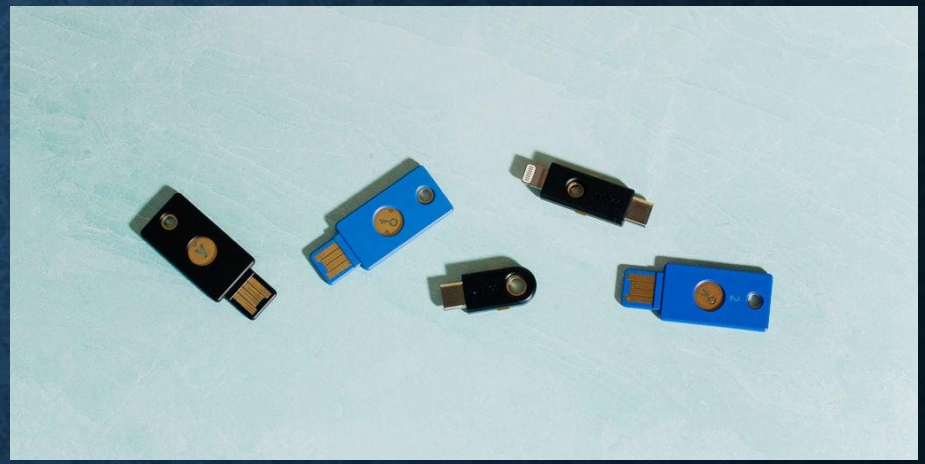
- **Viruses** are unauthorized programs that can annoy users, steal sensitive data or be used to control equipment that is controlled by computers.

THREATS TO INFORMATION SYSTEM SECURITY

- Computer Viruses
- Unauthorized Access
  - the standard convention is to use a combination of a username and a password. Hackers have learnt how to circumvent these controls if the user does not follow security best practices.
  - **Two-factor authentication.**

SOLUTIONS TO THREATS

- Anti-virus
- Network Firewall
- Data Encryption
- Physical Security Key
- Biometric Identification
  - Popular in smart phones, laptops



INFORMATION SYSTEMS ETHICS

- BCS (British Computer Society) Code of Conduct
  - The BCS Code of Conduct serves as a unique and powerful endorsement of your integrity and as a code of ethics for IT professionals.
  - Four Key principles
  - "You make IT for everyone"
  - "Show what you know, learn what you don't"
  - "Respect the organization or individual you work for"
  - "Keep IT real. Keep IT professional. Pass IT on."

OTHER CODE OF CONDUCTS

- ACM Code of Ethics and Professional Conduct
  - https://www.acm.org/code-of-ethics
- IEEE Code of Ethics
  - https://www.ieee.org/about/corporate/governance/p7-8.html