Course: Professional Issues in Information Technology

Week 12: Computer Misuse

Lecturer: Martha Gichuki

Learning outcomes Lecture 12:

Computer Misuse

At the end of this lecture, the learner should be able

to:

1. Describe the Computer Misuse Act
2. Describe the threat of insiders
3. Describe Espionage, Hacking and other forms of computer misuse
4. Describe the possible solutions to the problem of computer misuse

Course Description

- The course begins with an introduction to terminologies like profession, data and Information Technology. This will be followed by a coverage of the data processing cycle, an introduction to Law, Ethics and the Concept of privacy. Cyber crimes will then be covered to see what the law says in relation to cyber crimes.
- A detailed coverage of Intellectual property rights will then follow with the learners being exposed to various property rights and the glaring issue of plagiarism.
- The four dimensions of ethical dilemmas will then follow to enable learners apply wisdom in matters related to ethical decision making.
- An evaluation of the effect of Information Technology in employment will culminate the course where learners will cover issues related to health and safety at work, Netiquette, Software contracts, major internet security issues and Computer misuse.

Computer Misuse Act 1990: Introduction:

- Computer misuse - users access computers without permission, makes changes to files on a computer without permission or uses computers in ways that are considered unethical.
- The Computer Misuse Act makes it illegal to access computers in an unauthorized manner or damage to computerized information[1].
- Authorized users have permission to use certain programs and data. Whenever these users go beyond what is permitted, it is regarded as a criminal offence.
- The act makes provisions for accidentally exceeding permitted activities and also covers fraud, extortion, and blackmail.

1 Professional Issues in Information Technology. Bott, F. *British Computer Society, UK.* (2005) Pg. 175-178

Computer Misuse Act 1990 – Computer Misuse offenses

The Act contains three main offenses, summarized as follows: -

A person is guilty of an offense:-

1. Upon causing a computer to **perform any function** with the intention of **securing access to any program or data** held in a computer.
2. Upon intending to secure **access** to the computer while **unauthorized**.
3. Having knowledge that at the time when one causes a computer to perform the function, one is not an authorized user[2]

2. Professional Issues in Information Technology. Bott, F. *British Computer Society, UK.* (2005) Pg. 175

Computer Misuse offenses…

- It is illegal to access a computing system unless authorized to do so
- The activity of hacking is a crime regardless of whether the hacker is in a remote location, working from a distance over the remote area networks or locally.
- When persons such as employees or students who may have limited authorization use computers but knowingly exceed that authority[3].
- Hacking need not be directed at a particular computer, program or data.

3 Professional Issues in Information Technology. Bott, F. *British Computer Society, UK.* (2005) Pg. 177- 178

Computer Misuse offenses…

It is unlawful, without proper authorization:

i. To use another person's credentials to access a computer, use data or run a program

ii. To alter, delete, move or copy a program or data, or simply output a program or data

iii. To lay a trap to obtain a password.

- A person guilty of an offense shall be liable on summary conviction to imprisonment for specified terms or fines established by the government in place on the standard scale or both[4].

4 Professional Issues in Information Technology. Bott, F. *British Computer Society, UK.* (2005) Pg. 175

Examples of Computer Information portraying Confidentiality aspect.

1. Employer's confidential documents

- Any employee who copies his employer's confidential documents and then discloses them without authority to somebody else may both infringing the copyright in the documents.
- The employee is also said to be acting in breach of confidence, for which the employer can also sue[5].

5 Professional Issues in Information Technology. Bott, F. *British Computer Society, UK.* (2005) Pg. 180

2. Patient Information

- A doctor is supposed to keep his patients' information confidential.
- Patient information may only be disclosed it if permitted by the patient or authorized next of kin.
- Transborder data flows may carry patient information especially where patients are seeking treatment abroad[6]

6 Professional Issues in Information Technology. Bott, F. *British Computer Society, UK.* (2005) Pg. 180

3. Corporate Espionage

- Corporations at one time or another engage in offensive information warfare when they actively seek intelligence about their competitors' trade secrets through illegal means, such as bribing insiders.
- They sell information about their customers, sometimes violating their privacy.
- The main motivation is money and gaining a competitive position[7].

7 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 97

Misuse by insiders – Insider Threat

- Insiders consist of **employees, former employees, temporaries, contractors, consultants, suppliers, visitors, collaborators** and others with inside access to an organizations resource.
- Insider group is considered to be an organizations **biggest threat**.[8]
- Insiders act as information brokers, selling sensitive information belonging to their organizations to foreign governments, competitors, and organized crimes.

8 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 96

- Insider attacks are triggered by negative events in the workplace e.g. prior disciplinary issues
- Some of the insider attacks are planned in advance with most of them actioned from home.
- The motive behind insider attacks could be greed, disgruntlement, revenge, anger, excitement or divided loyalty among others[9]

9 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 96

Misuse by insiders …

- Insider actions compromise business and military plans, intelligence operations, and individual privacy.
- Insiders sabotage their employers' computer system and walk out with trade secrets to start competing firms.
- Insider attacks are motivated by money, ideology, revenge, and the desire to help the outsiders who exploit them[10]

10 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 96

Hackers

- These are people who gain access to or break into electronic systems, particularly computers and telecommunications systems.
- The motive of hackers includes thrill, challenge, and power.
- Many hackers do not seek financial reward when they damage the system they attack; however, others hack for money or to shut down computers[11].
- However, even when there is no malevolent intent, unauthorized hacking damages the integrity of the system and is more than a nuisance to system owners.

11 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 90, 95

Criminals

- Criminals target financial information resources such as **banks and credit card numbers or intellectual property that can be converted to money through underground sales**.
- They frequently operate within criminal enterprises (organized crime), but even individual criminals have succeeded in carrying out million-dollar heist.
- They are **mainly motivated by money**[12].
- This group includes information brokers and those who **sell pirated software, compact disks (CDs), and videos.**

12 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 90, 95

Government Agencies

- Several government agencies engage in offensive information warfare.
- Law enforcement agencies target the communications, records, and organizational structures of criminals to collect evidence and intelligence in criminal investigations[13].
- Intelligence agencies seek the military, diplomatic, and economic secrets of foreign governments, foreign corporations, and foreign adversaries.

13 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 113, 151

Government Agencies …

- Intelligence agencies draw easily on inside moles and electronic surveillance to supply information.
- Military units destroy adversary command and control information systems during times of war.
- Government regulators censor speech and restrict access to information technologies for national security and public safety objectives[14].

14 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 191

Terrorists

- Terrorists are of particular interest because of the potential damage that can result from attacks against critical infrastructure such as emergency services and financial systems.
- Terrorists collect information about their targets, spread propaganda, and sabotage physical equipment and buildings.
- There have been few reported cyber-attacks by terrorists[15].

15 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 99

Pornography

- Pornography refers to any material in form of writings or pictures dealing with sexual matters in a manner intended to incite lust, and therefore considered obscene.
- Pornography is a **description** or **portrayal of any activity regarded as obscene**.

Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 194

Pornography …

- Recently, pornography is also taking the format of movies and television where pornography of violence which is far more demoralizing than the pornography of sex is portrayed[16].
- Computer misuse in relation to pornography is widely practiced by the makers i.e. programmers of the computer software as well as the users[17].

16, 17 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 194, 196

How Programmers misuse computers in relation to pornography

a) Trickery:

- Through use of ordinary domain names such as Whitehouse.com, mighty Africa.com, Godscreation.com.
- These domain names trick innocent users to think that the sites are not pornography related while in actual fact they do.
- This translates to abuse of the users' conscience[18].

18 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 198

How Programmers misuse computers in relation to pornography …

b) Illegal computer operations:

- This is mostly done by changing the meaning of standard agreed upon widgets e.g. the close button.
- In some web sites it is actually used to open another page or site that has pornographic material[19].

19 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 196

How Programmers misuse computers in relation to pornography…

c) **Social engineering**[20]

- Computer users are tricked to register to gain access to pornographic site.
- In the process of registration, some details such as the credit card numbers are entered which in turn are used to fleece the user's Bank account[21].

20 Professional Issues in Information Technology. Bott, F. *British Computer Society, UK.* (2005) Pg. 164
21 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 195

How Programmers misuse computers in relation to pornography…

d)Misuse of **Computer memory:** - through usage of large storage space to store irrelevant material(s).

e)**Time Wastage**: A lot of useful time is spent accessing these pornographic sites leading to low productivity of workers and low profits or none at all.

f) **Network congestion**: Downloading graphics and video takes a lot of Bandwidth, which in turn congests the network and degrades your internet speed [22].

22 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 196

Effects of pornography to:

1. *Organizations*
   - Misuse of organizational productive time.
   - Jamming of the corporate internet/ communication lines.
   - Moral degradation.
2. *The Society*
   - Moral degradation.
   - Exposure of minors to sexual material
   - Low productivity of the affected individuals
3. *Individuals*
   - It's **addictive**, this leads to psychological slavery to pornography.
   - Pornography is also a high contributor to sexual pervasion e.g. **homosexuality, masturbation, fetishism** etc.
   - In case of a minor involvement by some adult(s), it could lead to **punishment by the law since i**t's illegal.
   - The individual could get **conned** by giving personal details to subscribe to a pornographic site[23].

23 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 62, 196

Solutions to the above effects

1. Packet filtering
2. Use of firewalls on the pornographic site
3. Taking disciplinary action (code of ethics)
4. Staff monitoring at the work place though the use of dataveillance and logs[24].

24 Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011) Pg. 63, 198

Technology and Privacy

- Users have personal information stored electronically and they would wish to have it availed over networks when needed.
- As technology evolves, privacy is threatened. Bits of transaction data left on websites can be used by the web site owner for commercial purposes or cause bigger harm.
- Another threat to privacy is databases containing "public" information e.g. **tax records, motor vehicles, drivers' licenses, convictions etc**. Such information is easily available to the general public through the Internet. This culminates to violation of an individual's privacy rights since it can be used for purposes outside the initial intention based on the individual's consent[25]

25 Professional Issues in Information Technology. Bott, F. *British Computer Society, UK.* (2005) Pg. 175

Invasion of Privacy in the computer Age

IT allows individuals, governments and businesses to invade the privacy of others.

When might invasion of privacy be justified?

- ✓**Building individual profile** - massive amounts of information stored in databases can be searched rapidly. However, governments and businesses are stockpiling information that should not concern them. A democratic society must find a balance between respect for individual privacy and freedom of information.
- ✓**Dataveillance -** This is the surveillance of personal data and computers can be used for real-time surveillance. Surveillance of individuals (personal surveillance) is a weapon in the fight against crime. However, it could provide a basis for coercion or blackmail. The aim of mass surveillance is to identify individuals that are worth subjecting personal surveillance.

Information Technology is not only a threat to privacy; it provides technical means to enhance one's privacy. For example:

1. **Encryption** for end-to-end confidentiality involving intermediate communications channels (public/private) subject to malicious intrusion. This enhances privacy and secure commerce.
2. **Anonymization** enables users to send and/or receive messages secretly making it very difficult to trace the identity of a user.
3. **Automated privacy-negotiation protocols**, such as the Platform for Privacy Preferences Project (P3P) that enable web site operators convey privacy policies in a special format that can be interpreted by clients linking to the web site. The clients recall the privacy preferences of their users, which are then compared with those of the visited web site and if they match, the connection is allowed; otherwise, user's attention is sought.

Content Covered in Lecture 12: Computer Misuse

We have been able to cover the following:

1. Described the Computer Misuse Act
2. Described the threat of insiders
3. Described Espionage, Hacking and other forms of computer misuse
4. Described the possible solutions to the problem of computer misuse

Course Text Books

1. Professional Issues in Information Technology. Bott, F. *British Computer Society, UK*. (2005)
2. Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA*. (2011)
3. Computers in Society: Privacy, Ethics and the Internet. George, J.F. *Pearson Prentice Hall, New Jersey.* (2004)
4. Cyber-ethics: Morality and Law in Cyberspace, 5th ed., Spinello, R.A. *Jones & Bartlett, Burlington, Mass., USA.* (2013)
5. Contemporary Issues in Ethics and Information Technology. *Schultz, R.A. IRM Press, USA*. (2005)