

Course: Professional Issues in Information Technology

Week 12: Computer Misuse

Lecturer: Martha Gichuki

Lecture learning outcomes

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

1.1 Introduction: Computer Misuse Act 1990:

- Computer misuse addresses users who access computers without permission, makes changes to files on a computer without proper 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 information¹.
- 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.

1.1.1 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.

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

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 user².
- ✓ 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 authority³.
 - ✓ Hacking need not be directed at a particular computer, program or data.

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 in this section shall be liable on summary conviction to imprisonment for specified terms or fines established by the government in place on the standard scale or both⁴.

1.1.2 Computer Information portraying Confidentiality aspect.

I. 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 sue⁵.

II. Patient Information

- ✓ A doctor is supposed to keep his patients' information confidential.

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

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

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

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

- ✓ Patient information may only be disclosed if permitted by the patient or authorized next of kin.
- ✓ Transborder data flows may carry patient information especially where patients are seeking treatment abroad⁶

III. 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 position⁷.

2.1 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 threat⁸.
- Insiders act as information brokers, selling sensitive information belonging to their organizations to foreign governments, competitors, and organized crimes. 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 others⁹. 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 them¹⁰.

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

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

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

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

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

2.2 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.

2.3 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 and they are mainly motivated by money¹².
- This group includes information brokers and those who sell pirated software, compact disks (CDs), and videos.

2.4 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.
- 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.

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

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

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

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

2.5 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 terrorists¹⁵.

3.1 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. 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 portrayed¹⁶.
- Computer misuse in relation to pornography is widely practiced by the makers i.e. programmers of the computer software as well as the users¹⁷.

3.1.1 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' conscience¹⁸.

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 material¹⁹.

c) Social engineering²⁰:

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

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

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

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

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

²⁰ Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA.* (2011) Pg. 195

- 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 account²¹.
- d) Misuse of **Computer memory**: Through usage of large storage space to store irrelevant materials.
- e) **Time Wastage**: A lot of useful time is spent accessing these pornographic sites.
- f) **Network congestion**: Downloading graphics and video takes a lot of Bandwidth, which in turn congests the network²².

3.1.2 Effects of pornography to:

❖ *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 it's illegal.
- ❖ The individual could get conned by giving personal details to subscribe to a pornographic site²³.

²¹ Professional Issues in Information Technology. Bott, F. *British Computer Society, UK.* (2005) Pg. 164

²² Ethics in Information Technology, 4th ed. Reynolds, G. *Course Technology, Boston, USA.* (2011) Pg. 195

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

3.1.3 Solutions to the above effects

- ✓ Packet filtering
- ✓ Use of firewalls on the pornographic site
- ✓ Taking disciplinary action (code of ethics)
- ✓ Monitoring of the staff at the work place²⁴.

4.1 Technology and Privacy

- Users have personal information stored electronically and they would wish to have it available over networks when need be.
- 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 aggregated to 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 and this may be viewed as a violation of an individual's privacy rights since it can be used for purposes outside the initial intention based on the individual's consent²⁵

4.1.1 Privacy Invasion in the computer Age

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

When might invasion of privacy be justified?

- To build a profile of an individual - massive amounts of information stored in databases can be searched rapidly. However, there is growing concern that 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.

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

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

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

1. **Encryption** provides end-to-end confidentiality when the intermediate communications channels are either public or, if 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). These 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. The user needs not read the privacy policies at every site he or she visits, but relies on the client for this task.

Content Covered in Week 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 and References

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)