INFORMATICS INSTITUTE OF TECHNOLOGY

TRENDS IN COMPUTER SCIENCE

MODULE 4COS008C

Legal, Social and Ethical concerns for Computer Scientists and Software Engineers

1.E LEGAL PROTECTION FOR INDIVIDUALS

NAME: Aathif Aslam

UOW NUM: W1954109

IIT NUM:20221079

GROUP MEMBERS:

1. Sandula Yasas -W1954018
2. Lahiru Dinusha – W1954026
3. Rehan Hansaja -W1954111
4. Aathif Aslam- W1954109

Contents

Table of figures

1.Introduction

As we all are aware, the technology is rising day to day becoming more and more inferior. The computer and other technological devices maybe seen as a tool for various purposes, making human work much efficient and effective.

Usage of such devices maybe threat to some and opportunity for another, but the technological evolution and invasion during these past generations has brought many impacts to the society and the individuals involved.

Figure 1 Usages of Technology

2. Legal methods to protect individuals

2.1 What activities need to be prevented?

Illegal activities commonly known as “crimes” performed through the technological devices are referred to as “**Cybercrimes**”. These can be of many types, some identified methods of performing crimes can be listed also whereas there are many unidentified ways yet to be discovered.

Due to the vast expansion of technology, crime rate has increased to a towering level among many users.

2.2 Common illegal activities

Information security is defined as “protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction,” (Federal Information Security Modernization Act, 2002).

Some of the Commonly committed cybercrimes are: -

1. Hacking
2. Phishing
3. Plagiarism
4. Cyber Harassment

2.2.1 Hacking

Hacking is considered as an act of stealing or entering to a technological portal where the is prohibited. In simpler words known as an unauthorized access to other individuals private or sensitive data or information. This could be done by an individual or group of individuals commonly referred to as “Hackers”. These attacks are also prone to confidential data or files stored by large industries.

2.2.2 Phishing

Phishing is the act of stealing sensitive information like bank account information or username and password credentials of individuals, or companies to achieve their goal.

Mostly, users are duped into entering these credentials by spam messages, spam emails and spam websites promising of major rewards which contents the viewers mind and heart.

2.2.3 Plagiarism

Plagiarism is the art of displaying or portraying one’s creation or innovation as another’s work. Due to this the originality of the innovation is denied, as there maybe more individuals claiming the innovation for themselves.

2.2.4 Cyber Harassment

Due to the expansion of communication through technology, many ways can be used to communicate with one another through means of technology. Mostly social media apps top the trend with the efficient and effective features that are inclusively provided within an app. A major reporting of cases relating to harassment, hate content, sexual harassment/abuse, religion offenses and racism can be seen in the present.

2.3 Commonly used preventive measures

1. Avoid entering sensitive information to unknown messages, emails etc.
2. Using of firewalls for extra network protection.
3. Obtaining patent rights, trade marks to own an innovation done by yourself.
4. Using of citations and referencing methods to quote and also to appreciate the work of learned authors/scholars.
5. Use of logical security like pins and passwords.
6. Updating to the newest versions of software so the bugs or loops are fixed.

Figure 2 Logical Security

3. Implications of Security Breach for a Company

3.1 What is Data Breach?

A data breach exposes confidential, protected data to unauthorized access and manipulation. (Joseph, 2018)

Data breaches are among the most important computer security and privacy problems. It is routine for the attackers to steal millions or even billions of records. Despite being such a massive problem, data breaches are considered outcomes of other security issues, such as human error and software vulnerabilities. In addition to severe security consequences, data breaches pose direct privacy issues; most data breaches reveal sensitive data to ill-intentioned people who sell it on the dark web and could release it publicly. (Saleem and Naveed, 2020)

3.2 Consequences of Data Breach to Companies

Data breaches are not only on the increase but firms struggle to detect, defend and respond to such breaches (Rosati, 2019)

Due to this companies' experience;

1. Disclosure of trade secrets
2. Falling of share prices
3. Loss of customer trust
4. Ruined business reputation
5. Financial losses and fine payments

3.3 Implication measures for a company

With data breaches now a common occurrence, it is becoming increasingly plain that while modern organizations need to put into place measures to try to prevent breaches (Kude ,Hoelle and Sykes ,2017)

1. Providing physical and logical security
   It is the duty of the technical staff to maintain physical security as well as logical security in order to stop data thefts from unauthorized access and hacking
   Eg: firewall, password, fingerprint motions

2. Educating and Training
   It is the duty of the employer to instruct and educate employees about the data breach and ways of implications. Also, the practice of Code of Ethics should be followed in a right manner.

3. Practical implications
   To remediate the risks and losses associated with data breaches, companies may use their reserved funds.

4. Social implications
   Company data breach announcements signal internal deficiencies. Therefore, the affected companies become liable to their employees, customers and investors. (Juma'h and Alnsour, 2020)

5. Encryption
   It is the method of ciphering and deciphering the confidential messages sent between a sender and a receiver, in order to prevent ethical misuse of data.

4. Critical Evaluation

According to the analysis of this report, cyber-crime has been reported in all parts of the world due to the misuse of technology for various purposes. There are many ways to legally protect ourselves from these type of crimes by adhering to the security implications as well as the code of ethics. If the guidelines are properly followed, we can convert the contaminated users of technology to proper ethical and legalized users, which is better for us and the society.

Figure 3 Data Breach

5. Conclusion

Today, many of us work with computers, play on computers at home, go to school online, buy goods from merchants on the internet, take our laptops to the coffee shop to read emails, use our smartphones to check our bank balances, and track our exercise with sensors on our wrists. In other words, computers are ubiquitous. (Andress, 2019).

We know that due to technological expansion in the present and in the upcoming future many threats have the possibility for occurrence.

As such it is our duty to maintain an ethical way of using technological devices and also to maintain security implications to protect our privacy.

(Word count= 1017)

Figure 4 Data Encryption

Acknowledgement

I would like to express my gratitude to the people who dedicated their valuable time to give their feedback relating to this course work. I would also wish to thank my lecturer, Prof. Prasad Wimalaratne and Ms. Sulari Fernando for their motivation and support to complete this course work within the given time period.

References

- Andress, J. (2019). *Foundations of information security.* San Francisco: No Starch Press, Inc. Available from https://learning.oreilly.com/library/view/foundations-of-information/9781098122546/xhtml/ch01.xhtml[Accessed on 30th oct 2022]

- government, US. (2002). Federal Information Security Modernization Act. 44: U.S.C 3542. Available from https://corpuslegalis.com/us/code/title44/cited/definitions7 [Accessed on 30th oct 2022]

- Joseph, R. (2018). Data Breaches: Public Sector Perspectives. *IT professional*, 57-64. Available from https://library-collections-search.westminster.ac.uk/discovery/fulldisplay?docid=cdi_proquest_journals_2087742493&context=PC&vid=44WST_INST:WST_VUA&lang=en&search_scope=MyInst_and_CI&adaptor=Primo%20Central&tab=ALL&query=any,contains,data%20breach&offset=30[Accessed on 1st nov 2022]

- Juma'h, A. and Alnsour,Y.(2020). The Effects of Data Breaches on Company Performnce. *International Journal of Accounting & Information Management*, Volume 28 Issue 2. Available from (through google scholar)https://www.ingentaconnect.com/content/mcb/ijaim/2020/00000028/00000002/art00004 [Accessed on 30th oct 2022]

- Kude,T. ,Hoelle,H.,Sykes,T.A. (2017). International journal of operations & production management. *Emerald Journals*, 57. Available from https://library-collections-search.westminster.ac.uk/discovery/fulldisplay?docid=cdi_gale_infotracmisc_A482170382&context=PC&vid=44WST_INST:WST_VUA&lang=en&search_scope=MyInst_and_CI&adaptor=Primo%20Central&tab=ALL&query=any,contains,data%20breach&offset=20 [Accessed on 1st nov 2022]

- Rosati, P. et al. (2019). Social media and stock price reaction to data breach announcements: Evidence from US listed companies. *Research in international business and finance*, 458-469. Available form https://library-collections-search.westminster.ac.uk/discovery/fulldisplay?docid=cdi_gale_infotracacademiconefile_A564424008&context=PC&vid=44WST_INST:WST_VUA&lang=en&search_scope=MyInst_and_CI&adaptor=Primo%20Central&tab=ALL&query=any,contains,data%20breach&offset=30 [Accessed on 1st nov 2022]

- Saleem,H. and Naveed, M. (2020). SoK: Anatomy of Data Breaches. *Proceedings on Privacy Enhancing Technologies*, 153. Available from(through google scholar) https://petsymposium.org/2020/files/papers/issue4/popets-2020-0065.pdf [Accessed on 30th oct 2022]

- Figure 1 Usages of Technology
- https://images.app.goo.gl/DWwuQ6pNsde3GRa29

- Figure 2 Logical Security
- https://www.mooc.org/blog/cybersecurity-and-computer-science-whats-the-connection

- Figure 3 Data Breach
- https://www.websitepulse.com/blog/data-breaches-how-to-handle

- Figure 4 Data Encryption
- https://www.thelawyermag.com/au/news/general/optus-breach-could-spark-novel-class-actions/423779