Name: Bisesh Shrestha

Student ID: **219570044**

Unit Code: CET324

Unit Title: Advance Cyber Security

Date: 05/06/2022

Acknowledgements

We would like to express our heartfelt gratitude to everyone who made it possible for us to complete this report. A special thanks to my subject teacher, whose stimulating suggestions and encouragement enabled us to coordinate my research..

Thank You

Sincerely,

Bisesh Shrestha

Abstract

This report is prepared with the purpose of providing knowledge about cybercrime to students. During its study, I came to know that cybercrime is increasing day by day. Since I had to know more about cyber security, I have collected the information from the journal, research paper, and conference paper and went thoroughly it. I've identified some activities, as well as some of the benefits of those activities, that a cyber-clinic might engage in to provide services to its stakeholders. As a result, the report provides a description of the cyber clinic.

University of Sunderland has established the Cyber clinic which provide awareness about cybercrimes to student, staff of university and other peoples is surround to the University of Sunderland. The clinic's goal is to build and evaluate a study's objective and teamwork surroundings to raise awareness of cybercrime within the local community and organizations, as well as to help them build resistance against it. The main goal of the cyber clinic is to offer advice to those who are concerned about cyber security and those who may have experienced a breach of cyber security. To achieve the clinic's goals and objectives, it engaged in three major parts of activity:

*Public participation and advice*: by providing guidance to vulnerable groups in the Sunderland community, with a main target on schools and colleges students, staff of university and other peoples is surround to the University of Sunderland through different medium such as face-to-face, social platforms, emails etc.

*Research*: The clinic will conduct a research with students, staff as well as those who have faced a breach of cyber security. Relating to their cybercrime problems and issues, and how they would like to receive cybercrime awareness guidance in the future.

Finally, The main goal of the project was to create a transferable model for implementing cybercrime awareness clinics that could be replicated in other locations by drawing on the experiences and outcomes of the advice and research threads. (Karagiannopoulos, 2019)

Concerns that may arise from the establishment of such a service, as well as issues concerning liability and any lawful and/or professional worries in the establishment of a cyber-clinic.

1. Professional’s lack of expertise and availability: whenever we want, without experts this course cannot be given into curriculum therefore courses security might decrease when taught by non-expertise.
2. Lack of industry response: while collecting data about the cyber breach many company may not be interested in providing their data so industry response is important for cyber clinic
3. Insufficient resources: insufficient resources is main problems. Resources helps in providing knowledge about certain data
4. Lack of awareness of universities: awareness should be provided by every university which helps in determining the level of basic cyber security knowledge among university students and to determine whether or not cyber security awareness program is required.
5. The absence of government involvement: government should get involve in spreading awareness program because government can help in budget management, resources management also. (Catota, 2019)
6. Students' disinterest in security: student should take interest in taking part in cyber clinic. They should know about the cybercrime, issue and threats which helps them to secure their personal data or devices. (McDonald, 2016)

The steps that individuals and organizations can take to protect themselves from cyber-attacks, as well as the advantages which such measures will provide.

***Training the staff***:

Many hacker get access of your data by sending fraudulent mails or certain links. Untrained eyes may be easily duped by links that appear to be genuine. Which is why staff training is so crucial. One of the most ways to safeguard against cyber-attacks and all forms of information breaches is to educate your employees on cyber-attack preventative measures and data security threats. They must complete the following tasks:

1. Double-check whatever links once having to click on them.
2. Check the email contact information contained in the received e - mail.
3. Use caution when emailing sensitive information. If a requirement appears odd, it is most almost certain so. Before replying to the requirement, it is best to confirm by phone with individual.

***Keeping software and systems fully up to date***

When software aren’t fully updated hacker will exploit the weaknesses to get access to the data. When they get access to those data it might be too late to take action to them so to prevent them from accessing data you have to update your system every time.

***Ensure Endpoint Protection***

Endpoint security safeguards networks which are remotely linked to computers. Smart phones, laptops, and computers linked to corporate systems serve as points of entry for security threats. These paths must be protected by highly specialized threat detection software.

***Install a Firewall***

There are various types of complex cyber security incidents, and new versions arise on a frequent basis, even sometimes resurfacing. Placing your network behind one firewall is amongst the most effective ways to protect yourself from a cyber-attack. A firewall system will prevent malicious activity on ones systems from causing damage.

***Backup your data***

If cyber-attack occurs and you have lost the data then you may face serious financial loss so backing up your data seems to be the key to avoid data loss and economic damage.

***Access to systems should be restricted.***

By giving access to authorized person then no outsider can gain the access to your data which will secure your data. Secure access control needs to employ policies and procedures to ensure consumers who they are and that they have appropriate access levels.

***Wi-Fi Security***

Hiding Wi-Fi and using security protocol is the safest way to secure your data because any computer can be harmed by joining to network.

***Employee personal accounts***

Providing personal account will help to reduce number of attack because by providing personal account they can only access to limited data only.

***Access Management***

Hacker may install malware software on company hardware that might compromise systems. Controlled permissions request and preventing staff from implementing or attempting to access documents on network are beneficial to network's security.

***Password***

Changing password frequenting using uppercase number and symbols will maintain protection against external and internal threats.

On the one hand, it appears that we have little option in the issue. Most victims are not centered on malicious programs and attacks many use laptops, smartphones, and systems for other purposes, therefore we must rely on experts to protect us. However, we must recognize that cyber security specialist faces unique ethical problems that the rest of us may never face. Confidentiality is a key ethics in cyber security. Because of the nature of the profession, security professionals will have connection with and help manage Information that is individual, secret, or sensitive information and therefore should be kept private and confidential. People in this sector may be tempted to reveal whatever interesting information those who discovered while operating an antivirus program over someone's hard drive, but that also may endanger that person’s life or individual growth. Another ethical issue that may appear redundant when discussing a cyber-security professional is security.  If we're all ready to follow effect of the type security protocols in our daily activities. That is the responsibility of a cyber security professional in terms of security. Most people may not consider it a big deal If those who leave their laptop unsecured or failed to maintain a scheduled upgrade, however, it could be a significant ethical failure for a cyber-security expert. They have a greater responsibility than anyone to keep phones, relevant information, and systems safe. In a complex relationship, privacy concerns are intertwined with cyber security concerns. Cyber security is meant to keep us safe from threats such as ransom ware and identity fraud, two different types of hackers that depend heavily on invading a user's data. Consider the following high-profile data breaches in recent months: Target's 70 million payment transactions have been stolen, as were Instagram's 87 million user records mishandled by Cambridge Analytical and Equifax's 143 million payment documentation were stolen by unauthorized people. Groups that collect individual data about customers are required by law to keep that data safe from hacker attacks. Sadly, the hacked organizations have been at least partially responsible for so many high-profile data theft. The hackers took advantage of a widely known weakness which should have been updated. However, if the organization's corporate processes for software updates were incomplete or have not been accompanied, the weakness would remain unprotected, allowing hackers to get busy stealing.

# Bibliography

Catota, F. E., 2019. Cybersecurity education in a developing nation: the Ecuadorian environment. *journal of Cybersecurity,* 5(1).

Karagiannopoulos, D. V., 2019. The Portsmouth Cybercrime. *The\_Portsmouth\_Cybercrime\_Awareness\_Clinic\_Project\_Key\_Findings\_and\_Recommendations,* pp. 1-2.

McDonald, C., 2016.