

**Early Bird**

**UNIVERSITY PREPARATION CLASS (UPC)**

**Subject Title: Academic Writing**

Assessment Weightage Type: 10% Of Our Total Module Grades

**Individual Report**

**The rising need for cybersecurity**

**Year Of Enrollment**

**2021**

Name Abinab K.C

Assignment Submission Date:01/07/2022

Word Count:1029

I confirm that I understand my coursework needs to be submitted online under the relevant module page before the deadline for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Abstract

There is a rising case of cybercrimes reported all around the world in these 2 to 3 years one of the reasons behind this may be the lockdown due to the worldwide spread of the virus as many people lost their job and had no option but to steal others’ money and soon. People had a lot of free time and this caused them to do cyberstalking as well. The purpose of this research is to find out the major causes of cybercrimes and to make the readers know the need for cybersecurity. In this research, I have listed some of the major cybercrimes ongoing in the world. Cyberstalking is the upmost most talked about crime as many people suffer from this what happens here is that a person is harassed online by the means of online platforms and this causes emotional breakdown, depression, and soon. I have talked about other crimes such as theft of property and pornography. I researched to know the world leaders such as the US and the UK have done to enhance their cybersecurity. At last, I concluded my research by listing out the solutions to cybercrimes as well as making people and younger generations aware of the types of cybercrimes and their effects.

Contents

[Assessment Weightage Type: 10% Of Our Total Module Grades 1](#_Toc121293991)

[Chapter 1: Introduction 1](#_Toc121293992)

[Chapter 2: Background 2](#_Toc121293993)

[Some of the forms of cybercrimes are: 2](#_Toc121293994)

[Cyberstalking 2](#_Toc121293995)

[Pornography 2](#_Toc121293996)

[Theft of property 2](#_Toc121293997)

[Chapter 3: Conclusion 3](#_Toc121293998)

[Figure 1: My pull 2](#_Toc121294889)

**A screenshot of a video game

Description automatically generated**

Figure : My pull

# Chapter 1: Introduction

In general term, cybersecurity refers to the security or protection of the devices such as computers, laptops, and, other devices which uses technologies such as AI, and the internet soon. Cybersecurity is not new to us and this has been a topic of discussion for several decades. In a recent study by Intelligence2 (Intelligence-squared), as many as 23 percent of professionals indicated that they believed the threat of cyber-war has been grossly exaggerated (June 8, 2010)1. Cyber security has become a hot topic in the present context countries such as the US and the UK announced their intention to categorize cyber-attacks as acts of war and announced a new $1 billion (USD) initiative to develop advanced militarized cyber-security abilities respectively (BBC US, June 1 (2011)) (BBC UK, June 1 (2011))2. Cyber-security is a challenge that extends beyond national boundaries and requires global cooperation with no single group, country, or agency claiming ownership, according to a 2009 report by the US Department of Homeland Security (Department of Homeland Security, 2009)3. Cyber security has been a major concern as most of the theft of electronic data leads to major loss of the company. Large companies such as Twitter also suffer from ethical hacking and endure huge losses Twitter to avoid the theft of their data also ensures that if someone finds a bug in their system they reward them with cash prizes, this system is called bug bounty.

# Chapter 2: Background

Cybersecurity is now considered a very important aspect of our life as it helps us to prevent different frauds in the online community. In our country Nepal there is no prevalence of online businesses such as cryptocurrency, and bitcoin, and soon this is still because the Nepal government considers these types of businesses as a threat to cybersecurity actually in this case Nepal government does not have enough resources to secure online business platform and the need of cybersecurity in Nepal is growing rapidly. Cybersecurity has become a major and common feature of many of the developing countries in the world. Countries invest hugely in cybersecurity and billions of dollars are used to strengthen the sector. If the next war happens the war will be fought through devices such as computers and other modern devices and it is necessary to keep in check to the world. One of the major reasons IT has become a global job provider is the rising need for cybersecurity. The rapid expansion of technologies is also creating and making cyber security more challenging as we do not present permanent solutions for the concerned problem. Although, we are actively fighting and presenting various frameworks or technologies to protect our network and information all of these protect the short term only. However, better security understanding and appropriate strategies can help us to protect intellectual property and trade secrets and reduce financial and reputation loss, Most of the time governments face difficulties due to inappropriate infrastructure, lack of awareness, and sufficient funding. The government bodies need to provide reliable services to society, maintain healthy citizen-to-government communications, and protection of confidential information (Everyone’s responsibility, 2010)4.

## Some of the forms of cybercrimes are:

### Cyberstalking

It is defined as an act that is frequently done by intruding into individuals’ personal life to cause distress, anxiety, and fear. Cyber Stalkers often take advantages of the internet which allow them to continue their activities without being detected. An intrusion is possible in individuals’ personal life by approaching their friend circle, and family members or sending fake letters and emails to the targeted persons electronically. This causes emotional breakdown, depression, and soon in the targeted person’s life (A Report before Committee on Equality and Non-Discrimination, June 2013)4.

### Pornography

Pornography refers to printed or video material such as books, magazines, photographs, and video clips that contain descriptions or show sexual organs or activity intended to encourage sexual excitement. More often the same person gets involved in the production, distribution, and downloading of pornography. The motivation behind production and distribution becomes to attain financial gain (International Journal of Computer Applications, 2015)4.

### Theft of property

Cybercrimes also include the theft of people’s property through online platforms. This type of robbery is one of the main cybercrimes reported to governmental bodies. Many hackers hack into the personal bank account of the user and steal their money, property papers, and soon. This is a major concern to the people as their money is also not safe in the safest place such as a bank.

Thomas J. Watson was a pioneer in the development of accounting and computing equipment used today by business, government, science and industry. He built a worldwide industry during his 42 years at IBM.

Mr. Watson was born in Campbell, N.Y., February 17, 1874. His first job was at age 18 as a bookkeeper in Clarence Risley's Market in Painted Post, N.Y. Later he sold sewing machines and musical instruments before joining the National Cash Register Company as a salesman in Buffalo. He eventually worked his way up to general sales manager. Bent on inspiring the dispirited NCR sales force, Mr. Watson introduced the motto, "THINK," which later became a widely known symbol of IBM .

# Chapter 3: Conclusion

The need for cybersecurity is a major concern and people have to take it seriously. Cybersecurity in general should be excelled and major funding for development should be done. People should be aware of cyber laws as well as what should be done and not be done. Cyber security alludes to the innovations and procedures intended to secure machines, systems, and information from unapproved get to, vulnerabilities and assaults conveyed through the Internet by digital offenders (IEEE, 2007)5. Computer security is becoming a real terror for the computer world. With malware becoming increasingly complicated, analysis of these programs is also very time-consuming. Malware authors use a range of evasion techniques to harden their creations against accurate analysis. An individual should be aware of the ongoing need for cyber security and should be eager to learn more about it. IT as a compulsory subject should be added to the school subjects and proper information should be spread among the students to make them aware of the different categories of cybercrimes and their punishments. Education the younger generation directly educates the upcoming generation. cybersecurity is a very buzzed topic and one interested can even consider this a professional option and can earn good money through it. In this modern day and age if you look at crimes through the use of electrical devices it is increasing to stop these educated people are required and cybersecurity personnel is very high in demand. Lastly, I would like to conclude that the awareness of cyber security education is very important and it should be taken for granted as a matter of concern.

References

Intelligence2, The Cyber War Threat Has Been Grossly Exaggerated. June 8, 2010. http://intelligencesquaredus.org/index.php/pastdebates/cyber-war-threat-has-been-grossly-exaggerated/ (Last Accessed: May 30, 2011).

US Pentagon to treat cyber-attacks as “acts of war.” (2011). *BBC News*. [online] 1 Jun. Available at: http://www.bbc.co.uk/news/world-us-canada-13614125 [Accessed 7 Jan. 2022].

The UK beefs up cyber warfare plans. (2011). *BBC News*. [online] 31 May. Available at: http://www.bbc.co.uk/news/technology-13599916 [Accessed 7 Jan. 2022].

Goutam, R.K., 2015. Importance of cyber security. *International Journal of Computer Applications*, *111*(7).

Moskal, S., Yang, S.J. and Kuhl, M.E. (2017). Cyber threat assessment via attack scenario simulation using an integrated adversary and network modeling approach. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 15(1), pp.13–29.