# UCCyber's scenario

Student's Name

Institution of Affiliation

Course Code and Title

Instructor Name

Due Date

## Abstract

The rapid advancement of the internet and related technologies has led to several cyber insecurities, such as cyber-attack.[1] Thus, the development of UCCyber's has contributed to the improvement of cybersecurity offering protection to people and organizations from different forms of cyber-attack and malicious software programs. This protection prevents data manipulation, corruption, and software damage, resulting in revenue loss to various organizations and individuals.


## Introduction

UCCyber I was initiated by Jill, Chris, and Leon, an engineering student at Canberra University, in 2019. They developed antivirus software meant to address cybersecurity issues in educational institutions. The UCEdusecure is still in the infancy stage and is expected to be launched by the end of 2021. cybersecurity is essential since the government, financial, military, and medical organizations collect and store confidential data on various servers. [1]Some of the data are sensitive, and in case they are accessed by an unauthorized individual, they can bring about adverse effects to the institution. The number of cyber attacks has snowballed in recent years. However, the organizations are coming up with sophisticated techniques of preventing the breach of any vital information.

## Major problems

[2]The organization experienced its major challenge which was stimulated by the Covid 19 pandemic .The lockdown prevented the developers and their employees to continue working in their offices. They tried implementing remote working but it was difficult since they had to keep track of the work progress. They spent a substantial amount of time debating on the project

which would be used in carrying out the actual work. The team struggled although the lockdown period which resulted into less work and low earnings. Since the company was not making a lot commercially during the lock down period, the employees started worrying if the organization would afford to pay them.

After the lockdown they met face to face in the office they took less time to develop a virus detection system but it was only 91% accurate. There was still dis agreement between the members on what should be done first. They agreed to improve the accuracy of the system but they lacked technical expertise to continue with the project. Its due to this reason that further disagreement erupted upon the team members on what should be done. Suggestions such as developing data backup software's and VPN were made by the members however after much deliberation they agreed to develop antivirus soft ware on the virus detection system.

## Proposed solutions to the problems

[2]Since the organization supply chain and channels were affected, they need to adjust the ecosystem and adopt new ways to cope with Covid 19 related issues. It would help if they considered the non-traditional collaborations with the investors' .revenue response, however, are not the only way for UCCyber to survive during the crisis. The best way of ensuring that the company stabilizes fast is to identify the project that needs to be prioritized. This may involve launching campaigns to win back customers, adjust prices, create flexible payment methods, and digitalize their process. It is also crucial for the company to act with urgency during the crisis period. Gradual recovery may not be a solution since they have to recover the time lost during the lockdown period. It is evident that the UCCyber team spent most of its time urging and disagreeing during the lockdown period as they attempted virtual meetings. After realizing the

software was only 91% accurate, the team needs to work harder to deliver since the software is expected to be launched in a few months.

To attract more users, UCCyber can lower the price[2] for their antivirus software, increasing the number of users purchasing the antivirus. Price discounts tend to attract more people, and individuals tend to renew their subscription. Other marketing strategies UCCyber can employ is offering a one month free trial period to new subscribers and offering an extra free month to their loyal subscribers. This strategy not only maintains the current subscriber but also brings in more traffic to the company resulting in the financial stability of the UCCyber Company.

## Analyses risks and ethical issues

[3]The basis of any security system is determined by moral principles of the people involved in the profession .Even though people are crucial to the solution they are also the cause of most problems. The employees should be made aware of their responsibility in making ethical decisions. Micro computer software's pose a great threat since there are many people using the soft ware .[4]Section 117 of copyright law which was amended in 1980 addresses the issue of backing up copies of the software. The software users have the right to create a back up copy of the software in the archieve. The UCCyber can provide free backup to their users to eliminate the need for the users to buy software's which are intended to defeat copy protection system and create back software's .[4]The copy right laws also include the law around leasing materials that the leaser may determine what the lease holder can do with the software. It is important for the company to join the battle against software piracy. Some large soft ware publishers have risked at least 1 million dollars for anti piracy movements and additional device protection. It would

help for the new organizations such as UCCyber to join the anti piracy movement to ensure that they secure complete copyright and protect the soft ware against piracy.

Trade secrets help in protecting something valuable and useful. The law helps in protecting the secret and the unique aspects of the idea leaving it known to the discoverer and his or her confidents .Since UCCyber antivirus system was developed by three engineering student this law will help them to keep the details among themselves to prevent information theft. Applying trade secret law is critical in computer field since any leaked information about either the software or the hard ware can give great advantages to the competitors.

In 2018 the business software alliance estimated that a proximately 37% of software's used on personal computers were not licensed, this translated to $46.3 billion lost revenues. This shows that many people are interested in pirating software's and content .Copyright violation comes inform of counterfeit programmes, server overuse and software licenses .once the software is pirated people use the technique of hard disk to install software's to their computers which are sometimes sold. To prevent privacy UCCyber can embrace patent, copyright and end user agreements .They can protect the software by using copyrights and patents. This creates a legal foundation for the business to protect its inventions .The end user agreement is also important since it defines what the customer can and cannot do with the software.

The UCCyber software owners can incorporate a water mark in the source code. The watermark can be hidden in the software and a can be used to prove ownership of the program when extracted. It also give traceability which can discourage piracy of the software.

[5]Obfuscation is a method of making the software code and intelligible to humans sometimes complex algorithms can be used to adjust the software code into anything else or to

make it look random. This technique has been used by several organizations and has been successful unfortunately Obfuscation is not a complete solution since with enough time the attackers can unearth the source code .Due to this reason Obfuscation is always used in conjunction with tamper proof software's .The tamper proof software protects the system against reverse engineering and modifications.

## Mitigation strategies on ethical issues

Since the organization's employees were affected by the changes during the covid-19 crisis, they should work hard to ensure that they restore the good work relationship and confidence. The company should diligently build an ethics program and cooperate it into the company's daily activities to build a robust ethical culture. With a strong ethics culture, all the employees are determined to do what is right and promote values. The leaders are key drivers of the company culture and are responsible for setting the tone in the organization. They should keep the employees informed about the different ethical issues and how they may impact them and the organization.

Trust and privacy are intertwined in [6] cybersecurity laws and ethics. Preservation of privacy depends entirely on trust between the developers and the organizational employees. Violation of privacy can pose a significant threat to security. Breaching of privacy affects trust and exposes the organization to the risk of losing security. Data privacy can be achieved by the use of social or technical solutions. The best way of achieving data privacy is by complying with the laws and regulations.

## Conclusion

Covid -19 pandemic has affected different businesses, including the UCCyber. The inability to access offices during the CK down period affected the productivity of the staff. After the lockdown, the company resumed work, but unfortunately, the software was not as effective and accurate as expected. To improve the efficiency of the software, the team should come up with concrete strategies and try to come to a common point of agreement on what they should do next. They should also incorporate a different method of data privacy protection to boost the confidence of software users and investors.

REFERENCE

[1] Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, 102248.

[2] Santoki, A., & PAREKH, D. M. H. (2020). Marketing Strategies during Covid-19. Marketing, 7(14), 2020.

[3] Beach, P. M., Mailloux, L. O., Langhals, B. T., & Mills, R. F. (2019). Analysis of Systems Security Engineering Design Principles for the Development of Secure and Resilient Systems. IEEE Access, 7, 101741-101757

[4] Litman, J. (2020). Revising copyright law for the information age. In The Internet and Telecommunications Policy (pp. 271-296). Routledge.

[5] Dong, S., Li, M., Diao, W., Liu, X., Liu, J., Li, Z., ... & Zhang, K. (2018, August). Understanding android obfuscation techniques: A large-scale investigation in the wild. In International Conference on Security and Privacy in Communication Systems (pp. 172-192). Springer, Cham

[6] Kosseff, J. (2017). Defining cybersecurity law. Iowa L. Rev., 103, 985.