FOUNDATION IN ARTS

COURSEWORK COVER SHEET

SUBJECT TITLE	**: INTRODUCTION TO COMPUTER SCIENCE**
SUBJECT CODE	**: PCSC001**
INTAKE	**: JULY 2022**
COURSEWORK TITLE	**: REVIEW 1 – INDIVIDUAL ASSIGNMENT**
COURSEWORK	**: 15%**

The objective of this assessment is:

- To evaluate student's understanding on technology concepts.
- To encourage students to think critically about the ways technology advancements can improve our daily lives.

Student Name: _____

Student ID : _____

Table of Contents

CYBERSECURITY

Introduction

Cybersecurity involves using advanced technology to secure data from being compromised by cyberattacks. Cybersecurity plays an integral part in lowering the risks of attacks on data carried out with the assistance of advanced technological techniques. These attacks can potentially provide unauthorized users access to personal or corporate information or systems. When individuals use internet-based platforms to share information, they are concerned about the security of the shared information. Even without factoring in the financial costs that will be incurred as a direct result of the attacks, a person or corporation may suffer reputational harm. Therefore this paper aims to expand on Cybersecurity by discussing its evolution, how the technology functions, the fields in which it is applied, and cybersecurity findings. It will also discuss cybersecurity success stories, risks and benefits, future developments, and ethical issues or controversies.

Evolution of Cybersecurity

Cybersecurity did not exist before computers and the internet. Hacking and viruses had no significance before the 1960s, but as technological advances and crimes progressed, Cybersecurity took center stage in human consciousness. Cybersecurity started with research where students were allowed to experiment with new computers in the late 1960s (Guo, 2021). Researchers thought this was a sort of cybersecurity method since if the computers had any vulnerabilities, the students would be able to access them. Students tried to "hack" further into these computer systems, enabling businesses to improve cybersecurity and protection systems. As computers gained popularity, many companies started buying them to store their data. The ARPANET's development in the 1970s signalled the start of internet cybersecurity (Guo, 2021). This happened when Bob Thomas created a harmless virus that went through ARPANET systems and was later removed by Ray Tomlinson using an antivirus. This event led to the advancement of malware detection, and the U.S. Air Force and other institutions created the first security systems.

Kevin Mitnick is credited for starting cybercrimes that led to numerous cyber-attacks making Cybersecurity a need more than ever. Cyber dangers increased, and high-profile attacks began to occur more regularly in the 1980s. This led to the government publishing papers to offer advice on security standards and measures, making Cybersecurity much more severe (Guo, 2021). Early in the 1990s, the internet became widely accessible, which caused a change in cybersecurity awareness. The proliferation of new malware and virus packages throughout this decade made it evident that Cybersecurity needed to be accessible to everyone. In the 2000s, cybercriminals had a wide range of hardware and software weaknesses to take advantage of. The threat posed by pervasive innovation changed with the advancement of technology (Guo, 2021). The Department of Homeland Security created the National Cyber Security Division in 2003 due to cyberattacks and the absence of reliable preventative measures.

How Cybersecurity functions

Cybersecurity distributes many levels of protection throughout all the networks, applications, and computers. Users need to have a fundamental understanding of data safety concepts such as using robust passwords, regularly backing up their data, and knowing the

signs of an attack for security to work effectively (Thames and Schaefer, 2017). It is essential for the company, its personnel, its processes, and its technology to be built to operate in concert with one another to establish a cohesive defense against the possibility of cyberattacks. Therefore, cybersecurity technologies that perform correctly will be possible to perceive, examine, and fix any potential vulnerabilities in systems before hackers or malicious programs can take advantage of them. When dealing with cyberattacks, organizations need to have a plan. It is necessary to ensure the safety of three primary entities, including endpoint devices, networks, and the cloud (Thames and Schaefer, 2017). Most of the time, anti-malware software, next-generation firewalls, email security solutions, and malware protection are security measures utilized to defend these companies.

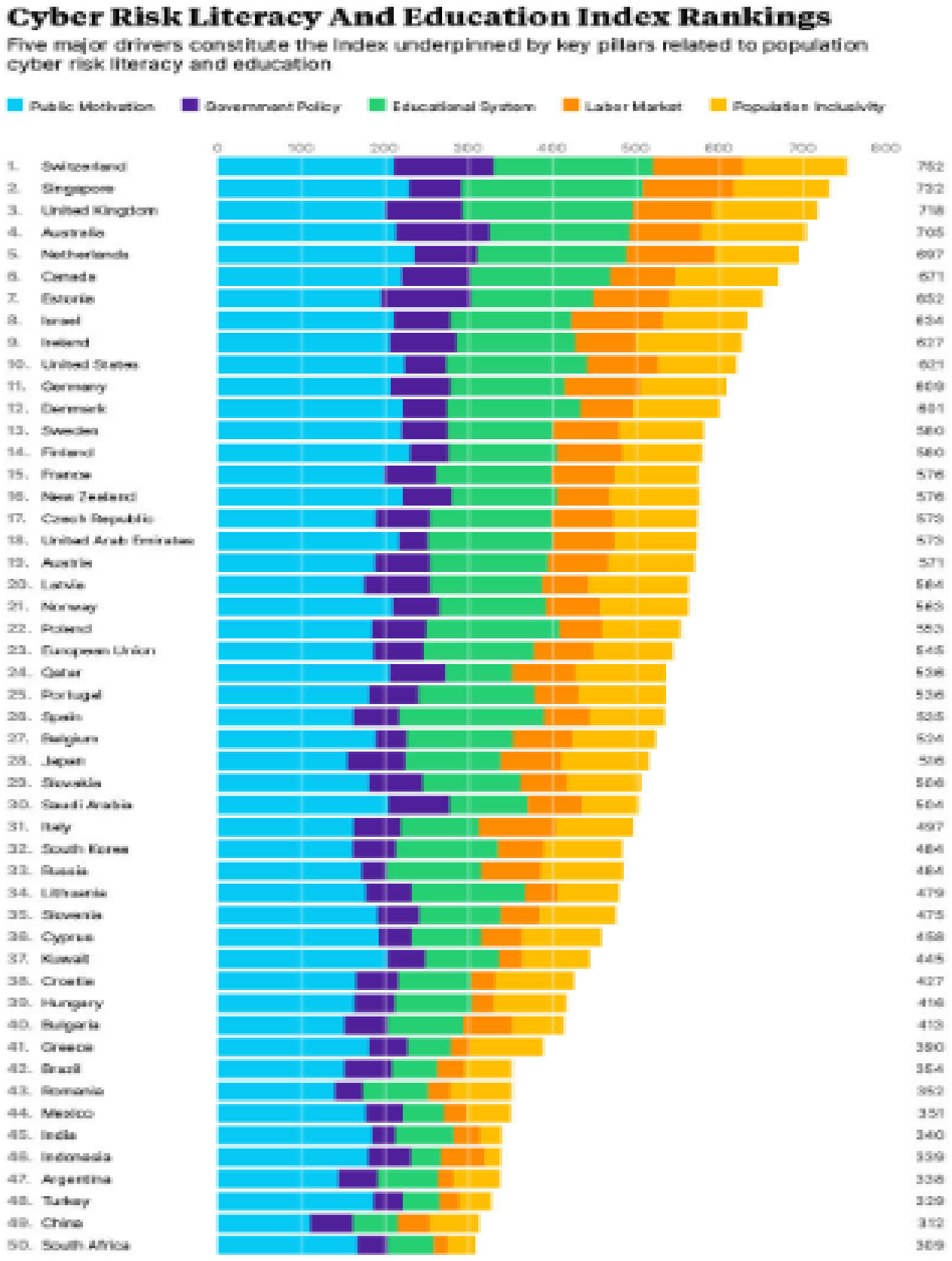
The fields in which Cybersecurity is applied.

Cybersecurity is required in almost every field, but it is evident that the need is most pressing in financial services, medical services, and government (Carter and Zheng, 2015). The potential applications of Cybersecurity are enormous in the financial services industry. Clients make payments online, make purchases online, and monitor financial accounts online, all of which create a significant risk for cyberattacks. Because they are required to store people's information, government entities are another sector in which Cybersecurity is employed. Because the information held by the government poses a threat to the country's safety if it falls into the wrong hands, the implementation of cybersecurity measures in this sector is essential for preventing potentially disastrous outcomes (Carter and Zheng, 2015). In the same way that the government is privy to a vast amount of confidential information, so are health care institutions. In addition, much like the government, they require Cybersecurity is designed to safeguard that data appropriately.

Cybersecurity Findings

The fight against cybersecurity is never-ending because there is no lasting, conclusive answer to the issue; as technology advances, so make the attacks (National Academies of Sciences, Engineering, and Medicine, 2014). The loss and harm that cybersecurity threats may cause can be significantly reduced by strengthening the existing knowledge and skills of individuals, businesses, government organizations, and the country. Users may question whether it is worthwhile to invest in security improvement if an adversary has the means to escalate the sophistication of its assault and the drive to persist even after numerous first attempts fail (Thames and Schaefer, 2017). However, waiting until perfect security can be implemented is undoubtedly a formula for passivity, leaving one open to several lower-level threats. Regrettably, human error is the root cause of the vast majority of breaches in cybersecurity. Ninety-five percent of security vulnerabilities result from negligence because of a skills gap in cybersecurity education. To this day, most governments' strategies for improving cybersecurity ignore the importance of continuing cyber-risk education for all of their citizens, regardless of age or socioeconomic demographic (Mee and Brandenburg, 2020). There are a lot of governments out there that publish their policies and their aspirational objectives, but not very many of them contain practical measures or consistent money to finish the job. The figure below shows fifty countries its government that has been working towards cyber risk education and awareness. The chart also demonstrates the five significant drivers that make up the index, which is supported by essential pillars connected to the literacy and education of the population regarding cyber risks.

Figure 1:



(Mee and Brandenburg, 2020)

Success stories of Cybersecurity

Using VAPT, an FMCG company situated in the United Arab Emirates, it improved its threat and risk mitigation by RNS Company. The organization uses Vulnerability Assessment and Penetration Testing VAPT (RNS Technology Services, 2021). It is a cybersecurity term encompassing many security tests intended to discover and mitigate cyber security risks. The client had an ongoing project with the security team, and the program's primary goal was to determine the current risk level in their system so that a suitable set of solutions could be put into action, which worked in the end. Another story is about how RNS found certain instances in which the management of access credentials in a leading insurance firm needed improvement. The client decided to start with a project to deploy, and that project concentrated on the employment cycle, user access, and the accreditation procedure (RNS Technology Services, 2021). The customer ultimately decided to go with SailPoint for the project after working with RNS. SailPoint IdentityIQ to allow agile deployment methodologies in several domains played a significant role in the decision-making process for the company. Using SailPoint, the insurance firm could strengthen its identity Governance.

Risks and benefits of Cybersecurity

Cyber security enhances virtual security, enhancing communication regardless of distance. It also boosts information security and expedites cyber data and the confidentiality of information for enterprises. It secures users' personal information, safeguards systems and infrastructure, and combats fraudulent activity and cybercriminals (Craigen, Diakun-Thibault, and Purse, 2014). Data breaches are a common cyber-attack that can have a significant negative impact on a corporation and can result from data that is not adequately protected. The prevalence of cloud services with lax default security settings and global connections increases the possibility of cyberattacks from within or outside the company.

Cybersecurity Future developments

A.I. and Machine Learning will have an ever-increasing and unceasing impact on the development of cybersecurity. Due to the dynamic nature of the online environment, security will inevitably progress over time (Carter and Zheng, 2015). Security must move away from adhering to a predetermined structure and instead be more evolutionary and self-sufficient. Training programs and customization will enable systems to recognize new dangers and respond appropriately. The advent of new hybrid cloud settings calls for a new method of cyber protection that puts algorithms and automation technologies to work protecting sensitive data (Carter and Zheng, 2015). Adopting intelligent SOCs that can automatically forecast, identify, prevent, and respond to threats is becoming increasingly common among businesses that are moving away from traditional security techniques.

Cybersecurity Ethical issues

A breach of someone's privacy could eventually have negative repercussions causing privacy harm. Theft of one's identity is one of the most common ethical privacy breaches online (Thames and Schaefer, 2017). If an individual exposes critical personal details, they open themself up to the risk of receiving pricey spam, phishing scams, and other unwanted users. The inevitably high cost of cyber security is an issue that will always be a factor in ethical considerations about the profession of cyber security. According to Thames and

Schaefer (2017), maintaining cyber security requires the participation of a significant number of people and a significant amount of organizational resources, including time, money, and skill; the associated cost is substantial. Costs will be considerably more significant if insufficient measures to protect against cyberattacks are in place.

Conclusion

The need for cyber security will only grow as the globe continues to become more interconnected through telecommunication networks transporting important transactions. In addition, it is also one of the essential components of the rapidly developing digital world. It is necessary to acquire the skills necessary to protect against attacks and educate others in these skills. This is because the attacks in the digital realm continue to be a persistent danger to computer networks. Despite the advancement of more improved security measures, criminals are growing more inventive, taking new and unique approaches, and launching fresh attacks. Therefore people and firms have no choice but to devise appropriate preventative measures and recovery strategies to combat the attacks.

References

Carter, W. A., & Zheng, D. E. (2015). *The evolution of cybersecurity requirements for the U.S. financial industry*. USA: Center for Strategic and International Studies.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10).

Guo, J. (2021).The Evolution of Cybersecurity: Where Did This All Begin? https://www.cybher.org/2021/11/22/the-evolution-of-cybersecurity-where-did-this all-begin/

National Academies of Sciences, Engineering, and Medicine. 2014. At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues. Washington, DC: The National Academies Press. https://doi.org/10.17226/18749.

RNS Technology Services. (2021). Customer Success Stories; Innovating the future of security. https://www.rnstechnology.com/success-stories/

Thames, L., & Schaefer, D. (2017). *Cybersecurity for industry 4.0*. Heidelberg: Springer.

Mee, P., & Brandenburg, R. (2020). Cybersecurity; After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk. https://www.weforum.org/agenda/2020/12/cyber-risk cyber-security-education

Task 1

Topic	Poor 1	Average 2	Good 3
Organization **(Overall order, flow, and transitions)**	Details and examples are not organized, are hard to follow and understand.	Information is scattered and needs further development.	Information is logicall ordered with paragraph transitions.
Quality of Information	Unable to find specific details.	Details are somewhat sketchy.	Some details don't sup report topic.
Introduction	Introductory paragraph is not apparent.	Introductory paragraph is vague.	Introductory paragraph clearly stated with a fo
Conclusion	Concluding paragraph is not apparent.	Concluding paragraph is only remotely related to the report topic.	Concluding paragraph and summarizes the re discussion and draws a conclusion.
Grammar & Spelling & Bibliography	Numerous grammatical and/or spelling errors. Resources not cited in paper or proper format not used.	Three to five grammatical or spelling errors. Some resources are cited but not all. Not formatted correctly.	Fewer than 3 grammat spelling errors. All res are cited, but formattin correct.