

Group Project Assignment Report

by Gabriel Florin Burcea

Submission date: 10-Jan-2025 08:32PM (UTC+0000)

Submission ID: 248001268

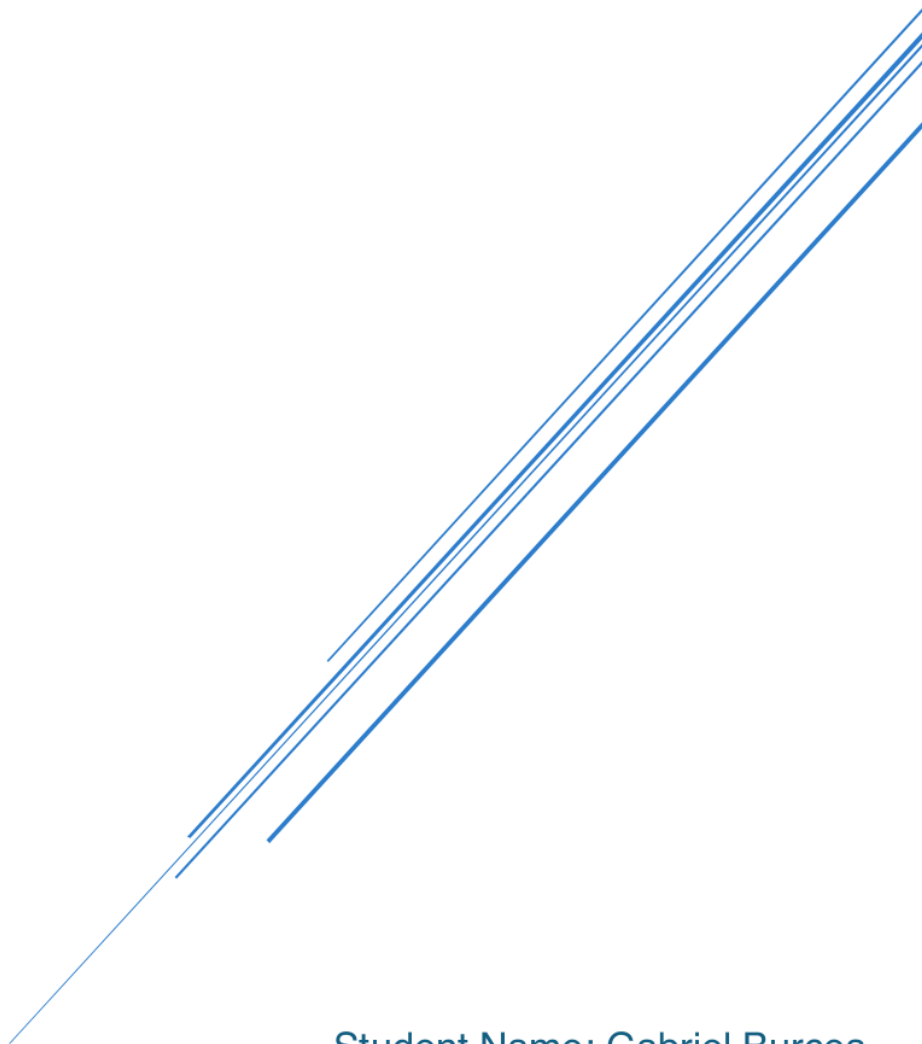
File name: 53445_Gabriel_Florin_Burcea_Group_Project_Assignment_Report_638742_199401693.docx
(3.16M)

Word count: 1937

Character count: 10953

CYBER SECURITY THREATS

Personal Data Breach Report



Student Name: Gabriel Burcea
Student ID: 2325506
Module: Group Project (ACBA4014)
Lecturer: Redwan Al-amri

Contents

Introduction 1

 Background 1

Main Body 3

 Literature review 3

 Methodology, aims and objectives of the project 3

 Potential result..... 4

 Project lifecycle..... 6

Conclusion 7

 Team performance 7

 Own reflection..... 8

 Information & Education is the key 8

Bibliography 9

Introduction

Background

Technology continues to shape our daily lives, the need for strong cyber security has become more urgent than ever. Cyber threats are evolving at an alarming rate,

targeting individuals, businesses, and governments with increasingly sophisticated tactics. Recognizing this growing challenge, our team chose to focus on cyber security threats for this project. Our goal is to analyse these threats, understand their impact, and explore solutions to raise awareness and improve protection against them.

This report searches into the key findings of our research, shedding light on the frequency and complexity of cyber-attacks and the vulnerabilities they exploit. We examine their effects on personal privacy, financial stability, and even national security. By studying real-world examples, we aim to uncover patterns and root causes, enabling us to develop practical solutions to mitigate these risks.

Central to our approach is the importance of awareness. Many cyber incidents reduce from a lack of understanding about potential threats, such as phishing scams, ransomware, and social engineering. By implementing awareness programs and sharing best practices, we aim to empower individuals and organizations to take proactive measures to secure their digital environments.

This project is a collective effort (students in class) to raise a more informed and resilient digital community.



Main Body

Literature review

As we rely more on digital platforms, the importance of strong cyber security becomes undeniable. Research highlights that both individuals and organizations face significant vulnerabilities in today's connected world. Two notable studies on this topic are "Cybersecurity: Protecting Critical Infrastructures" by Smith E (2022) and "Human Factors in Cybersecurity" by 2 Cyber-security specialists Patel and Kumar (2021). [1]

E. Smith focus on the rise of cyber threats like malware, ransomware, and phishing attacks. He explains how hackers often take advantage of weak passwords, outdated software, and poorly secured networks. The study highlights the need for regular updates and stronger security features, such as two-factor authentication, to prevent breaches.

Patel and Kumar, on the other hand, explore how human behaviour contributes to cyber risks. They discuss common mistakes like clicking on suspicious links, oversharing personal details, or ignoring basic security measures. The authors stress that educating people about these risks is just as important as improving technology.

Together, these studies show that cyber security is about more than just technology it's also about awareness. Addressing both technical gaps and human errors is essential to build better defences against modern cyber threats. [2]

Methodology, aims and objectives of the project

Our team of 5 students at the University of Wales Trinity Saint David adopted a **quantitative research** methodology for this project. This approach allowed us to gather and analyse numerical data to better understand the scope and impact of existing cyber security threats and vulnerabilities. By focusing on measurable data, such as the frequency of cyber-attacks, the types of vulnerabilities most exploited, and the behaviours that lead to breaches, we were able to identify key patterns and trends in cyber threats.

The primary objective of our research was twofold. First, we aimed to explore the most prevalent cyber security threats and understand how they exploit vulnerabilities in technology and human behaviour. This included studying real-world examples, reviewing statistical data, and identifying the areas where individuals and organizations are most at risk.

Second, our goal was to create an accessible and practical solution to address these issues. To achieve this, we developed an online course designed to educate individuals on how to protect themselves in the digital world. The course focuses on

raising awareness about common threats, such as phishing and ransomware, and provides actionable tips for safeguarding personal and professional data.

By combining quantitative analysis with a practical educational tool, we hope to empower individuals with the knowledge and skills needed to navigate the online world securely and confidently.

The frequency and severity of data breaches have surged in recent years, posing significant risks to individuals and organizations alike. These breaches often expose sensitive information, leading to identity theft, compliance violations, and damaged reputations. Understanding the statistics behind these incidents highlights the scope and impact of this growing threat.

In 2024, the average cost of a data breach reached a record \$4.88 million, underscoring the financial toll these events can take. Human error remains a leading cause, responsible for 88% of cybersecurity breaches, with 68% involving a human element. Alarming, it takes an average of 194 days to identify a breach and 292 days to contain it, giving attackers ample time to exploit vulnerabilities.

Identity theft remains a significant issue, with the Federal Trade Commission receiving over 1.1 million reports in 2022. Breaches increased by 72% in 2023 compared to 2021, highlighting the rising trend in cybercrime. Despite the risks, 64% of Americans have never checked if they were affected by a breach, and 56% are unsure of how to respond if their data is compromised.

Global factors also contribute to the rise in cyber threats, with 97% of organizations reporting increased attacks since the Russia-Ukraine conflict in 2022. Cyber fatigue, a growing issue, affects 42% of companies, leading to diminished proactive defense efforts.

These statistics emphasize the urgent need for increased awareness and robust security measures to combat the ever-growing risks of cybercrime. [3]

Potential result

The primary goal of our project is to educate individuals about cyber security and reduce the chances of being hacked. By increasing awareness of common threats and teaching practical defence strategies, we aim to allow people to take proactive steps to protect themselves in the digital world. Education plays a critical role in addressing the human factor in cyber security, which is responsible for 88% of breaches. When individuals understand how to recognize phishing scams, create strong passwords, and secure their online accounts, they become less likely to fall victim to cyber-attacks.

Through our online course, we hope to bridge the knowledge gap that leaves many people vulnerable. By addressing common mistakes and providing clear guidance on

best practices, the course is designed to equip users with the tools they need to navigate online spaces safely. Additionally, raising awareness can help reduce the growing problem of cyber fatigue, encouraging individuals to remain vigilant and engaged in protecting their digital lives.

If successful, this initiative has the potential to significantly lower the number of successful cyber-attacks. A well-informed population can not only protect personal information but also contribute to a more secure digital environment overall. [4]



Project lifecycle

The lifecycle of our project is designed to ensure continuous impact and long-term effectiveness in combating cyber threats. The initial phase involves the development of an engaging and informative online course that educates individuals about common cyber threats, such as phishing, ransomware, and social engineering. Once the course is created, it will be launched and made accessible to individuals and organizations seeking to improve their cyber security awareness.

To maintain its effectiveness, the course will not be a one-time effort. Cyber threats are constantly evolving, and staying updated is crucial. As part of the project lifecycle, we propose that this course becomes a mandatory refresher for users every six months or at least annually. These regular updates will serve as timely reminders and introduce users to the latest trends and tactics employed by cybercriminals. By keeping participants informed about emerging threats and reinforcing good security practices, this recurring education will help reduce complacency and cyber fatigue, which are significant vulnerabilities in maintaining robust security.

The feedback from users will be collected and analysed after each session to refine and improve the course content. This iterative process ensures that the course remains relevant, engaging, and effective. Ultimately, by incorporating regular updates into the project lifecycle, we aim to foster a culture of continuous learning and vigilance, significantly lowering the risk of cyber-attacks for individuals and organizations alike.



Conclusion

Team performance

In my opinion, our team worked well on this project, demonstrating strong collaboration, dedication, and a clear understanding of the importance of cyber security. Each member brought different skills and perspectives to the table, allowing us to create a comprehensive and practical project course aimed at educating individuals about cyber threats. We remained focused on our objectives, from researching the latest vulnerabilities to designing a course that is both informative and easy to follow.

I truly believe that our efforts will lead to a successful project, making a real difference in helping people protect themselves in the digital age. Cyber security is not just a technical subject; it's a critical aspect of our daily lives, especially as we continue to rely more heavily on technology. I hope this project serves as a reminder of how essential it is to stay informed and vigilant.

By demonstrating education and regular updates, I'm confident that we can contribute to creating a more secure online environment. I also hope that our work inspires others to prioritize cyber security as a key topic in both personal and professional settings, ensuring it remains a vital focus for years to come.

Own reflection

Looking back on this project, I am personally satisfied with the team performance. From the start, we were all committed to discuss the important issue of cyber security, and that drove us throughout the project. Personally, I learned a lot about the different types of cyber threats and how vulnerable people are, often due to simple mistakes like using weak passwords or falling for phishing scams. It was eye-opening to realize how easily these small actions can lead to major consequences.

What I enjoyed most was working with my teammates. Each of us brought something different to the table, which made our project even stronger. Building the online course was especially rewarding, as it felt like we were creating something that could help people protect themselves in their digital lives.

Reflecting on the project, I feel hopeful that it will make a real impact. Cyber security is such a crucial part of our everyday lives, and I believe everyone should take it seriously. This project made me even more convinced that education is the key to making a difference. I hope our course helps people stay safer online and sparks more discussions about the importance of cyber security. This experience has been incredibly valuable, and I'm proud to have been part of a team working on such an important issue.

Information & Education is the key

Cybersecurity information and education are crucial in today's digital world. As cyber threats become more sophisticated, individuals and organizations must be equipped with the knowledge to protect themselves. Awareness about common risks, such as phishing, malware, and data breaches, can help prevent costly and damaging attacks. Education empowers people to recognize vulnerabilities, adopt best practices, and stay updated on evolving threats. By fostering a culture of security, we can reduce human error, which remains a leading cause of cyber incidents. Ultimately, informed individuals are better prepared to navigate the digital world safely and securely.



Thank you for all the lessons throughout the module and I am confident that all the information will be a solid rock in building up my future and to develop in my career.

Best regards,

Gabriel

Bibliography

- [1] E. Smith, "Cibersecurity in today`s world," *Cibersecurity: Protecting Critical Infrastructures*, 04/2022.
- [2] P. &. Kumar, "Cybersecurity," *Human Factors in Cybersecurity*, 2021.
- [3] R. Sobers, "Cibersecurity Statistics," *Cibersecurity Statistics and trends updated 2024*, 13/09/2024.
- [4] S. Sjouwerman, "Security awarness training," *Stanford Research: 88% Of Data Breaches Are Caused By Human Error*, 03/03/2024.



Group Project Assignment Report

GRADEMARK REPORT

FINAL GRADE

38 / 100

GENERAL COMMENTS

Engagement with Literature (3/5%)

The literature review demonstrates an understanding of key sources, but it lacks depth and critical analysis. Greater engagement with recent studies would improve this section.

Knowledge and Understanding (14/20%)

The aims and objectives are well stated; however, some areas lack clarity and specificity. A more structured presentation of goals would enhance understanding.

Cognitive and Intellectual Skills (12/20%)

The methodology is explained but lacks thorough justification for the chosen approach. Stronger reasoning and critical evaluation of alternative methods would improve this section.

Practical Skills (6/10%)

Practical implementation is described, but additional details on execution and challenges faced would strengthen the report.

Transferable Skills (3/5%)

The report is well-structured, but referencing inconsistencies need to be addressed for better academic communication.

Overall

Good effort with clear objectives and relevant content. Focus on critical analysis, clarity, and referencing improvements for a higher grade. However, this was supposed to be a group project, and you were supposed to work with your group team!

Report Score: 38/60

Presentation Score: 0/40

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11
