

Group project assessment

by Gabriel Florin Burcea

Submission date: 03-Apr-2025 10:41PM (UTC+0100)

Submission ID: 254730554

File name: 53445_Gabriel_Florin_Burcea_Group_project_assessment_659667_47825535.docx (420.87K)

Word count: 2263

Character count: 13545



Prifysgol Cymru

Y Drindod Dewi Sant

University of Wales

Trinity Saint David

CYBERSECURITY THREATS

Personal Data Breach

Gabriel Burcea



CERTHE Group Project for CerTHE (ACBA4014)

YEAR 2024-2025

University of Wales Trinity Saint David

DECLARATION

I declare that this thesis entitled “*CYBERSECURITY THREATS: Personal Data Breach*” is the result of my own research except as cited in the references. The thesis has not been accepted to any degree and is not concurrently submitted in candidature of any other degree.

Signature : GB

Name of Student: Gabriel Burcea

Date : 31/03/2025

Contents

DECLARATION	1
-------------------	---

CHAPTER 1: Introduction	3
Research Background	3
Problem Statement	3
Research Questions and Objective	3
Significance of the Study	4
Definition of Terms	5
CHAPTER 2: Literature review	5
Cybersecurity risk types.....	5
Phishing.....	6
Malware	6
Data breach	8
Social Engineering.....	8
CHAPTER 3: Research Methodology	8
CHAPTER 4: Data Analysis	8
Review	9
CHAPTER 5: Discussion and Conclusion	10
Discussion	10
Conclusion.....	10
References	10

CHAPTER 1: Introduction

Research Background

This report explores our research findings on cyber-attacks, focusing on how often they happen, how complex they are, and the tactics hackers use. We look at the weaknesses they exploit and the damage they cause, from invading personal privacy to threatening financial security and even personal safety. By analysing today's world cases, we aim to spot common patterns and understand why these attacks happen. This helps us come up with practical ways to reduce the risks and protect against cyber threats.

Problem Statement

A crucial aspect of our approach is raising awareness. Many cyber incidents occur due to a lack of understanding of threats such as phishing, ransomware, and social engineering. As a result, people face an increasing risk of personal data breaches, leaving them vulnerable to identity theft, financial fraud, and privacy violations. Many individuals lack a clear understanding of how their data is exposed and the measures needed to protect it. Given these challenges, this research systematically examines the types of cybersecurity risks that lead to personal data breaches and explores how these risks vary across different online activities, industries, and digital platforms. By understanding these threats, we can identify gaps in security awareness and develop strategies to help individuals safeguard their personal information more effectively.

While past research, such as Firoozi & Mohsni (2023), has examined overall risk disclosure practices, there has been limited focus on cybersecurity-specific risks or the use of advanced analytical methods to analyse them in depth.

This thesis fills these gaps by conducting an in-depth analysis of personal data breaches across various industries and digital platforms, using both qualitative and quantitative methods to provide deeper insights into the risks and their impact. [1]

Research Questions and Objective

The objective of this thesis is to examine how personal data breaches impact individuals across different demographics and online activities. This research aims to identify the most common types of personal data breach risks people face, analyse how these risks vary across different digital platforms and industries, and explore

how factors such as age, digital literacy, and online behaviour influence exposure to these threats. Ultimately, the study seeks to provide actionable recommendations to improve awareness, enhance data protection practices, and empower individuals to safeguard their personal information more effectively.

The research questions are as follows:

1. What are the most common personal data breach risks individuals face?
2. How do personal data breach risks vary across different demographics, digital platforms, and industries?

Significance of the Study

This research explores different types of personal data breaches and how they impact various demographics, digital platforms, and industries. By identifying patterns and vulnerabilities, it provides important insights into the factors that put personal information at risk. Understanding these risks can help individuals and organizations take better precautions to prevent data breaches.

The study aims to raise awareness about personal data security and encourage safer online habits. By highlighting common threats and weaknesses, it promotes stronger cybersecurity practices that can protect people from identity theft, fraud, and privacy violations.

As we increasingly rely on digital platforms, strong cybersecurity is more essential than ever. Research shows that both individuals and organizations face serious risks in today's digital world. Two key studies on this topic are ***Cybersecurity: Protecting Critical Infrastructures*** by Smith (2022) and "***Human Factors in Cybersecurity***" by cybersecurity experts Patel and Kumar (2021). [2]

Smith's study focuses on rising cyber threats like malware, ransomware, and phishing. He explains how hackers take advantage of weak passwords, outdated software, and poorly protected networks. His research highlights the importance of regular updates and security features like two-factor authentication to prevent attacks.

On the other hand, Patel and Kumar examine how human behaviour contributes to cybersecurity risks. They point out common mistakes, such as clicking on suspicious links, sharing too much personal information, and ignoring basic security precautions. Their study emphasizes that educating people about these risks is just as important as technological advancements.

Together, these studies highlight that cybersecurity isn't just about technology it also depends on awareness and smart online habits. To strengthen defences against cyber threats, we must address both technical weaknesses and human errors. [3]

Definition of Terms

1. **Personal Data Breach** – A security incident that results in unauthorized access, disclosure, or loss of personal information, potentially leading to identity theft, financial fraud, or privacy violations.
2. **Cybersecurity** – The practice of protecting systems, networks, and data from cyber threats, including hacking, phishing, and malware attacks.
3. **Data Privacy** – The right of individuals to control how their personal information is collected, stored, and shared by organizations or digital platforms.
4. **Identity Theft** – A type of cybercrime where an individual's personal information is stolen and used fraudulently, often for financial gain.
5. **Phishing** – A cyber-attack method where attackers deceive individuals into providing sensitive information, such as passwords or credit card details, by posing as a trustworthy entity.
6. **Ransomware** – Malicious software that encrypts a victim's data, demanding payment in exchange for restoring access.
7. **Social Engineering** – Manipulative tactics used by cybercriminals to trick individuals into revealing confidential information or performing actions that compromise security.

CHAPTER 2: Literature review

Cybersecurity risk types

Cybersecurity risks are diverse and can be classified into several categories, each presenting distinct challenges to general population and organisations. This study explores five major types of cybersecurity threats: malware, phishing, ransomware, denial-of-service (DoS) attacks, and insider threats. Each section provides an in-depth analysis of these risks, their potential impact, and key research insights.

Phishing

Phishing is a common online scam where attackers pretend to be trusted companies or people to steal personal information. These scams usually happen through emails, social media, or fake websites that trick people into giving away passwords, credit card details, or other sensitive data. Cybercriminals often create messages that look real, using urgent warnings or fake offers to get quick responses.

The problem with phishing is that traditional security tools, like spam filters and blacklists, can't always catch these scams because attackers constantly change their tactics. They design emails and websites that closely resemble legitimate ones, making them hard to spot. To stay protected, people need to be cautious about unexpected messages, verify sources before clicking links, and use security features like two-factor authentication. Businesses and individuals can also benefit from AI-powered detection tools and cybersecurity education to recognize and avoid phishing attempts. Awareness and proactive steps are key to staying safe online.

In 2020, A.K. Jain and B. B. Gupta conducted an extensive study on phishing detection methods and found that machine learning techniques, particularly those analysing text and URLs, are far more effective than traditional security measures. Their research highlighted those conventional methods, such as blacklists and rule-based systems, struggle to keep up with evolving phishing tactics. In contrast, machine learning models can adapt to new threats by identifying patterns in fraudulent emails and websites. Their findings emphasize the need for advanced, AI-driven security solutions to enhance phishing detection and better protect users from falling victim to these cyber threats. [4]

Malware

Malware is a type of malicious software designed to infiltrate, damage, or disrupt computer systems. In the financial sector, such attacks can cause major disruptions, data breaches, and significant financial losses. Financial institutions must disclose these risks to maintain transparency and inform investors about potential threats.

According to the 2018 Verizon Data Breach Investigations Report, malware was involved in around 30% of data breaches. Many of these incidents were internet-based, targeting corporations and high-value individuals. With cybercriminals constantly refining their tactics, stronger security measures and proactive risk management are essential to minimize the impact of malware attacks.

Common Types of Malwares article by Tal Zamir (Tech Expert)

1. Viruses

Viruses attach themselves to clean files and spread through a computer, corrupting data and potentially deleting files. They remain dormant until an infected file is executed.

2. Worms

Worms spread automatically by exploiting system vulnerabilities. They can slow down networks and overwhelm system resources.

3. Fileless Malware

This advanced malware operates from system memory, making it harder to detect. It exploits legitimate system tools rather than installing files.

4. Spyware

Spyware secretly collects personal data, including passwords and financial details. It often comes bundled with software or through deceptive links.

5. Adware

Adware shows unwanted ads and may track browsing habits. While not always harmful, it can be annoying and slow down your system.

6. Trojans

Trojans disguise themselves as legitimate software but allow hackers to access your system. They don't replicate like viruses but can be just as harmful.

7. Rootkits

Rootkits give attackers deep access to a system and are difficult to detect. They can modify security software and reinstall themselves after removal.

8. Ransomware

This malware locks your files and demands a ransom to restore access. It spreads through phishing emails or security vulnerabilities.

9. Keyloggers

Keyloggers record keystrokes to steal passwords and financial information. They often enter systems via malicious downloads or infected email attachments.

Tal Zamir, a tech expert with 20 years in the industry, knows how to tackle big business challenges with smart technology. As he mentioned in this article, he advises keeping antivirus software updated and staying alert to online threats to keep your data safe from hackers and malware. [5]

Data breach

A data breach occurs when unauthorized individuals access or steal sensitive information, such as personal details or financial records. These breaches can result from cyberattacks, malware, phishing scams, or even employee mistakes. The consequences can be severe, including financial losses, reputational damage, and legal issues.

Strong preventive measures like multi-factor authentication and advanced encryption help protect sensitive data. Staying vigilant, updating security systems, and educating employees about cyber threats are crucial in minimizing risks.

Social Engineering

Social engineering is a growing cybersecurity threat, especially in the financial sector, where sensitive data is highly targeted. Instead of hacking systems directly, attackers manipulate people to bypass security measures. Common tactics include phishing, pretexting, and baiting, which exploit trust and lack of awareness to gain unauthorized access.

CHAPTER 3: Research Methodology

This research developed a quantitative and qualitative methodology to analyse cybersecurity threats and vulnerabilities. By examining attack frequency, exploited weaknesses, and human behaviours, key trends were identified.

The study had two objectives: first, to explore major cybersecurity threats and their exploitation of technology and human error; second, to develop an online course educating individuals on digital security, focusing on threats like phishing and ransomware. Data breaches have surged, with the average cost reaching \$4.88 million in 2024. Human error accounts for 88% of breaches, with detection taking 194 days on average. Strengthening awareness and security measures is essential to mitigating risks. [6]

CHAPTER 4: Data Analysis

Descriptive analysis is a technique used to summarise and outline the key characteristics of a dataset. It involves calculating statistical measures such as mean, median, mode, standard deviation, and frequency distributions, which offer a clear overview of cybersecurity risks and trends. This method provides a simple way to understand the data's main features and identify general patterns.

In this paper we present the results of a survey that examined the attitude of users to cybercrime as well as their awareness of cyber security threats. The study was conducted among Israeli and Slovenian students. [7]

Name of a variable	Question / Description	Total	IL	SI	T
		Mean (SD)	Mean (SD)	Mean (SD)	
Awareness	Are you familiar with the term cyber security? (1-no knowledge to 4-very good knowledge)	2.44 (.81)	2.39 (.84)	2.57 (.60)	T= 1.10 p>0.05
Familiarity	Familiarity with different sources? (the variable represents an average of 9 tools)	3.98 (.81)	3.56 (1.91)	4.85 (2.36)	T= 3.83**
IT future	Would like to attend IT security training? (1-definitely not to 5-definitely yes)	3.74 (.97)	3.65 (1.0)	3.97 (.85)	T=1.66 ¹
Threats	The main cyber security threats are? (the variable represents an average score from 14 options)	4.04 (.87)	4.06 (.88)	4.00 (.86)	T= -.35, p>0.05
Effect of education on awareness	The extent to which the current education influenced their cyber-security awareness? (1-definitely not affected to 5-strongly affected)	3.22 (.98)	3.15 (.90)	3.40 (.95)	T=1.29, p>0.05
Provide or find on the Web?	Total sum of the amount of information that the responders provide or find in the Web (1-strongly disagree to 5-strongly agree)	2.42 (.93)	2.54 (.90)	2.13 (.95)	T= -2.19*
Computer skills and knowledge	Self-evaluation of skills and knowledge in using computer application (1-no skills to 5-very high skills)	3.22 (.67)	3.25 (.70)	3.16 (.60)	T=.62, p>0.05
Behavioral	I know how to behave in case of a cyber attack (1-definitely no to 5-rather yes)	3.10 (1.19)	3.07 (1.19)	3.17 (1.20)	T=.66, p>0.05
Choice	Is the use of technology products coming from your desire or by coercion? (1-definitely by coercion to 5-definitely by choice)	3.22 (1.00)	3.40 (.98)	3.11 (1.02)	T=1.46, p>0.05
Protection	Sum of the score in the usage that the responders make to protect their instrument (the variable represent an average of 11 option of procedures that can be used to protect their devices)	4.09 (2.23)	3.50 (1.87)	5.60 (2.39)	T=5.16***
Length	The average length of your standard password (minimum 0 to maximum 14 characters)	9.43 (5.27)	8.99 (5.72)	10.49 (3.85)	T=1.41, p>0.05
Finish	The variable represents an average of 5 processes that can be taken when finishing working of the computer.	1.37 (.73)	1.32 (.67)	1.48 (.88)	T=1.08, p>0.05

Review

Through a review of various articles, we found that cyber threats present significant risks to untrained individuals across different industries and general users. Without proper knowledge and precautions, these users are highly vulnerable to cyberattacks, making them prime targets for data breaches, financial loss, and identity theft.

CHAPTER 5: Discussion and Conclusion

Discussion

This study examines the disclosure of personal data breaches from the perspective of general users. Timely and clear communication is essential to protect individuals from identity theft and financial loss. The research highlights the need for improved user awareness and standardized breach disclosure practices to ensure timely action and protection.

Conclusion

This thesis examined cybersecurity risk disclosures for general users and companies using descriptive analysis. Our findings revealed that common risks, such as data breaches, phishing, ransomware, and malware, are frequently disclosed, highlighting shared cybersecurity threats for both individuals and organizations.

References

- [1] M. F. & S. Mohsni, "Cybersecurity disclosure in the banking industry: a comparative study," *International Journal of Disclosure and Governance*, Vols. Palgrave Macmillan, vol. 20, pp. 451-477, 2023.
- [2] K. & Patel, "Cybersecurity," *Human Factors in Cybersecurity*, 2023.
- [3] E. Smith, "Cybersecurity in today's world," *Cybersecurity: Protecting Critical Infrastructures*, 04/2022.
- [4] A. K. J. & B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges," *Enterprise Information Systems*, 08 July 2020.
- [5] T. Zamir, "What is Malware?," *Common Malware Examples and Types You Should Know About*, 2021.

[6] S. Sjouwerman, "Security awarness training," *Stanford research: 88% of data breaches are cause by human error*, 03rd of March 2024.

[7] D. Lesjak, "SURVEY," *CYBER SECURITY AWARENESS AMONG STUDENTS: A COMPARATIVE STUDY IN ISRAEL AND SLOVENIA*, September 2019.

Group project assessment

GRADEMARK REPORT

FINAL GRADE

69 / 100

GENERAL COMMENTS

1. Engagement with Literature (5%)

Awarded Marks: 4/5

The literature review section demonstrates a good engagement with relevant sources, including both academic studies and expert commentary. Studies such as Jain & Gupta (2020), Smith (2022), and Patel & Kumar (2021) are appropriately referenced to support the discussion on phishing, human error, and cyber threats. The student also used expert insights (e.g., Tal Zamir) to strengthen practical understanding. However, the range of academic sources could be slightly expanded to include more peer-reviewed, recent journal articles for a higher mark.

Feedback:

You have effectively cited relevant literature to support your arguments, especially in the literature review and significance sections. To further improve, integrate more up-to-date peer-reviewed sources and critically engage with differing viewpoints in the field.

2. Knowledge and Understanding (20%)

Awarded Marks: 16/20

The report reflects a strong understanding of the topic, with clear articulation of the problem, objectives, and significance. The explanation of cybersecurity issues is well-structured and demonstrates a logical flow from background to specific research questions. The student clearly understands the social and technical dimensions of cybersecurity risks.

Feedback:

You've presented a thorough and well-structured introduction and problem statement. The objectives and significance of the study are clearly aligned with your research questions. For higher marks, aim to deepen the theoretical underpinnings by linking

your discussion more explicitly to cybersecurity frameworks or models.

3. Cognitive and Intellectual Skills (20%)

Awarded Marks: 14/20

There is evidence of analytical thinking in the literature review and in the selection of methodologies (qualitative and quantitative). The justification of research design, however, is brief and could benefit from a more rigorous explanation of how the methods align with the research objectives. The discussion lacks deeper critical engagement with the data and alternatives to the chosen approaches.

Feedback:

You demonstrated sound reasoning in method selection and linked some of your methodological choices to the study's aims. To score higher, expand on the justification for using mixed methods and include a more critical evaluation of the methodology's limitations.

4. Practical Skills (10%)

Awarded Marks: 6/10

The research includes a practical component (survey) and analysis of user attitudes, showing that the student has applied research in practice. However, there is little detail about the research design (e.g., sampling strategy, data collection process), and data analysis is quite general. More precise application of statistical or thematic analysis methods would strengthen this section.

Feedback:

Your report shows some practical application through the survey, which is commendable. To further enhance this section, provide more detail about how the research was conducted and analyzed, including tools used and how findings were validated.

5. Transferable Skills for Life and Professional Practice (5%)

Awarded Marks: 4/5

The student has communicated the research findings clearly and in an organized manner. The report is well-structured, with appropriate headings, citations, and references. Language and tone are generally academic. A few grammatical errors and slight repetition in some areas detract from clarity but do not obscure meaning.

Feedback:

You've communicated your findings effectively and used appropriate academic referencing. For full marks, proofread your report to eliminate minor language issues and refine the structure for conciseness and impact.

Report : 44/60

Presentation 25/40

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12
