

Higher Nationals

Internal verification of assessment decisions – BTEC (RQF)

INTERNAL VERIFICATION – ASSESSMENT DECISIONS			
Programme title	BTEC HND in Computing		
Assessor	Mr. Lilanka	Internal Verifier	
Unit(s)	Unit 13: Computing Research Project		
Assignment title	Final Research Report – Remote working		
Student's name	Ryan Wickramaratne (COL 00081762)		
List which assessment criteria the Assessor has awarded.	Pass	Merit	Distinction
INTERNAL VERIFIER CHECKLIST			
Do the assessment criteria awarded match those shown in the assignment brief?	Y/N		
Is the Pass/Merit/Distinction grade awarded justified by the assessor's comments on the student work?	Y/N		
Has the work been assessed accurately?	Y/N		
Is the feedback to the student: Give details: • Constructive? • Linked to relevant assessment criteria? • Identifying opportunities for improved performance? • Agreeing actions?	Y/N Y/N Y/N Y/N		
Does the assessment decision need amending?	Y/N		
Assessor signature		Date	
Internal Verifier signature		Date	
Programme Leader signature (if required)		Date	

Confirm action completed			
Remedial action taken Give details:			
Assessor signature		Date	
Internal Verifier signature		Date	
Programme Leader signature (if required)		Date	

Higher Nationals - Summative Assignment Feedback Form

Student Name/ID	Ryan Wickramaratne (COL 00081762)		
Unit Title	Unit 13: Computing Research Project		
Assignment Number	1	Assessor	Mr. Lilanka
Submission Date	12/08/2023	Date Received 1st submission	
Re-submission Date		Date Received 2nd submission	

Assessor Feedback:

LO2 Conduct and analyse research relevant to a chosen computing research project

Pass, Merit & Distinction Descriptors

P3 ☐ P4 ☐ M2 ☐ D1 ☐

LO3 Communicate the outcomes of a research project to identified stakeholders

Pass, Merit & Distinction Descriptors

P5 ☐ M3 ☐ D2 ☐

LO4 Reflect on the application of research methodologies and concepts

Pass, Merit & Distinction Descriptors

P6 ☐ P7 ☐ M4 ☐ D3 ☐

Grade:	Assessor Signature:	Date:
Resubmission Feedback:		
Grade:	Assessor Signature:	Date:
Internal Verifier's Comments:		
Signature & Date:		

* Please note that grade decisions are provisional. They are only confirmed once internal and external moderation has taken place and grades decisions have been agreed at the assessment board.

Assignment Feedback

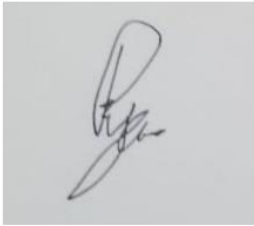
Formative Feedback: Assessor to Student

Action Plan

Summative feedback

Feedback: Student to Assessor

Date

Assessor signature			
Student signature	 ryandilthusha@gmail.com	Date	

Pearson Higher Nationals in Computing

**Unit 13: Computing Research Project
Project Report**

General Guidelines

1. A Cover page or title page – You should always attach a title page to your assignment. Use previous page as your cover sheet and make sure all the details are accurately filled.
2. Attach this brief as the first section of your assignment.
3. All the assignments should be prepared using a word processing software.
4. All the assignments should be printed on A4 sized papers. Use single side printing.
5. Allow 1" for top, bottom , right margins and 1.25" for the left margin of each page.

Word Processing Rules

1. The font size should be **12** point, and should be in the style of **Time New Roman**.
2. **Use 1.5 line spacing**. Left justify all paragraphs.
3. Ensure that all the headings are consistent in terms of the font size and font style.
4. Use **footer function in the word processor to insert Your Name, Subject, Assignment No, and Page Number on each page**. This is useful if individual sheets become detached for any reason.
5. Use word processing application spell check and grammar check function to help editing your assignment.

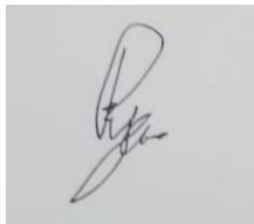
Important Points:

1. It is strictly prohibited to use textboxes to add texts in the assignments, except for the compulsory information. eg: Figures, tables of comparison etc. Adding text boxes in the body except for the before mentioned compulsory information will result in rejection of your work.
2. Avoid using page borders in your assignment body.
3. Carefully check the hand in date and the instructions given in the assignment. Late submissions will not be accepted.
4. Ensure that you give yourself enough time to complete the assignment by the due date.
5. Excuses of any nature will not be accepted for failure to hand in the work on time.
6. You must take responsibility for managing your own time effectively.
7. If you are unable to hand in your assignment on time and have valid reasons such as illness, you may apply (in writing) for an extension.
8. Failure to achieve at least PASS criteria will result in a REFERRAL grade .
9. Non-submission of work without valid reasons will lead to an automatic RE FERRAL. You will then be asked to complete an alternative assignment.
10. If you use other people's work or ideas in your assignment, reference them properly using HARVARD referencing system to avoid plagiarism. You have to provide both in-text citation and a reference list.
11. If you are proven to be guilty of plagiarism or any academic misconduct, your grade could be reduced to A REFERRAL or at worst you could be expelled from the course

Student Declaration

I hereby, declare that I know what plagiarism entails, namely to use another's work and to present it as my own without attributing the sources in the correct form. I further understand what it means to copy another's work.

1. I know that plagiarism is a punishable offence because it constitutes theft.
2. I understand the plagiarism and copying policy of Edexcel UK.
3. I know what the consequences will be if I plagiarise or copy another's work in any of the assignments for this program.
4. I declare therefore that all work presented by me for every aspect of my program, will be my own, and where I have made use of another's work, I will attribute the source in the correct way.
5. I acknowledge that the attachment of this document signed or not, constitutes a binding agreement between myself and Pearson , UK.
6. I understand that my assignment will not be considered as submitted if this document is not attached to the assignment.



ryandilthusha@gmail.com

12/08/2023

Student's Signature:
(Provide E-mail ID)

Date:
(Provide Submission Date)

Higher National Diploma in Computing

Assignment Brief

Student Name /ID Number	Ryan Wickramaratne (COL 00081762)
Unit Number and Title	Unit 13 – Computing Research Project
Academic Year	2021/22
Unit Tutor	Mr. Lilanka
Assignment Title	Final Research Project Report
Issue Date	
Submission Date	
IV Name & Date	

Submission format

- The submission is in the form of an individual written report.
- The submission is in the form of an individual written report.
- This should be written in a concise, formal business style using single spacing and font size 12.
- You are required to make use of headings, paragraphs and subsections as appropriate, and all work must be supported with research
- referenced using the Harvard referencing system.
- Please provide a referencing list using the Harvard referencing system.
- The recommended word limit is minimum 4,500 words

Unit Learning Outcomes:

- LO2.** Conduct and analyse research relevant to a chosen computing research project
LO3. Communicate the outcomes of a research project to identified stakeholders
LO4. Reflect on the application of research methodologies and concepts

Assignment Brief and Guidance:

Learner is now required to provide a comprehensive research project report based on the findings of secondary and primary research carried out on the project proposal submitted in the previous section on Remote working.

The Learner requires to produce a detailed research project report covering following areas

- Conduct primary and secondary research using appropriate methods for a computing research project that consider costs, access and ethical issues. Carry out your research and apply appropriate analytical tools to analyse research findings and data and discuss merits, limitations and pitfalls experienced during data collection and analysis.
- Draw conclusion based on the research findings.
- Communicate the outcomes of your research project to the identified audience and a critical evaluation of the outcomes demonstrating if the research objectives were met.
- Reflect on the success of your research project and your performance at the end of the project with the inclusion of a project evaluation and recommendations (Consider alternative research methodologies and lessons learnt in view of the outcomes)

--	--

Grading Criteria	Achieved	Feedback
P3 Conduct primary and secondary research using appropriate methods for a computing research project that consider costs, access and ethical issues		
P4 Apply appropriate analytical tools to analyse research findings and data.		
M2 Discuss merits, limitations and pitfalls of approaches to data collection and analysis.		
P5 Communicate research outcomes in an appropriate manner for the intended audience.		
M3 Coherently and logically communicate outcomes to the intended audience, demonstrating how outcomes meet set research objectives.		
D2 Communicate critical analysis of the outcomes and make valid, justified recommendations.		
P6 Reflect on the effectiveness of research methods applied for meeting objectives of the computing research project.		
P7 Consider alternative research methodologies and lessons learnt in view of the outcomes.		
M4 Provide critical reflection and insight that results in recommended actions for improvements and future research considerations.		
D3 Demonstrate reflection and engagement in the resource process leading to recommended actions for future improvement.		

List of figures

FIGURE 1 LIONS RESTORATION COMPANY	17
FIGURE 2 SOME WELL-KNOWN BUSINESSES THAT HAVE LATELY EXPERIENCED SECURITY INCIDENTS	20
FIGURE 3 WAYS TO DEFEND AGAINST PHISHING ATTACKS.....	21
FIGURE 4 WAYS TO PREVENT INSIDER DATA THEFT	23
FIGURE 5 WAYS TO PREVENT THIRD PARTY VENDOR ATTACKS	24
FIGURE 6 SURVEY RESULT FOR QUESTION 8	25
FIGURE 7 THE NUMBER OF EMPLOYEES RECRUITED EACH YEAR WITH OR WITHOUT REMOTE WORKING EQUIPMENT BY THE COMPANY.....	26
FIGURE 8 PAST EMPLOYEE DESKTOP SCREEN SHOT WITH HAVING COMPANY AND PERSONAL DATA MIXED UP.....	27
FIGURE 9 NUMBER OF EMPLOYEES USED THEIR CORPORATE EMAIL FOR UNAUTHORIZED WEB SITES AND NOT	28
FIGURE 10 COST SHEET ON EQUIPMENT REPAIRS AND MAINTENANCE FOR REMOTE WORKERS.....	29
FIGURE 11 RESEARCH ONION	48
FIGURE 12 PRESENTATION OF DATA FOR ENTIRE QUESTION 1- DO YOU HAVE ACCESS TO COMPANY-SENSITIVE DATA IN YOUR REMOTE WORK?	66
FIGURE 13 PRESENTATION OF DATA FOR ENTIRE QUESTION 2- AREN'T YOU CONFIDENT ABOUT THE SECURITY MEASURES IN PLACE TO PROTECT COMPANY-SENSITIVE DATA WHILE WORKING REMOTELY?	67
FIGURE 14 PRESENTATION OF DATA FOR ENTIRE QUESTION 1- DO YOU BELIEVE THAT COMPANY-SENSITIVE DATA IS LIKELY TO BE EXPOSED DUE TO REMOTE WORKING?	68
FIGURE 15 PRESENTATION OF DATA FOR ENTIRE QUESTION 1- DO YOU FEEL YOU AND YOUR FELLOW EMPLOYEES ARE NOT WELL-TRAINED TO PROTECT COMPANY-SENSITIVE DATA IN A REMOTE WORK ENVIRONMENT?	69
FIGURE 16 PRESENTATION OF DATA FOR ENTIRE QUESTION 1- DO YOU FREQUENTLY PROVIDE PERSONAL INFORMATION FOR WORK-RELATED TASKS WHILE WORKING REMOTELY?.....	70
FIGURE 17 PRESENTATION OF DATA FOR ENTIRE QUESTION 1- AREN'T YOU CONFIDENT ABOUT THE SECURITY MEASURES IN PLACE TO PROTECT YOUR PERSONAL DATA WHILE WORKING REMOTELY?	71
FIGURE 18 PRESENTATION OF DATA FOR ENTIRE QUESTION 1- DO YOU BELIEVE THAT YOUR PERSONAL DATA IS LIKELY TO BE EXPOSED DUE TO REMOTE WORKING?	72
FIGURE 19 PRESENTATION OF DATA FOR ENTIRE QUESTION 1- DO YOU FEEL YOU AND YOUR FELLOW EMPLOYEES ARE NOT WELL-EDUCATED ABOUT PROTECTING PERSONAL DATA IN A REMOTE WORK ENVIRONMENT?	73
FIGURE 20 PRESENTATION OF DATA FOR ENTIRE QUESTION 1- HOW FREQUENTLY HAVE YOU EXPERIENCED SYSTEM CRASHES WHILE WORKING REMOTELY?	74
FIGURE 21 PRESENTATION OF DATA FOR ENTIRE QUESTION 1- AREN'T YOU CONFIDENT IN THE COMPANY'S ABILITY TO QUICKLY ADDRESS SYSTEM CRASHES THAT OCCUR DURING REMOTE WORK?	75
FIGURE 22 PRESENTATION OF DATA FOR ENTIRE QUESTION 1- DO YOU BELIEVE SYSTEM CRASHES COULD LIKELY LEAD TO SECURITY ISSUES IN A REMOTE WORK ENVIRONMENT?	76
FIGURE 23 PRESENTATION OF DATA FOR ENTIRE QUESTION 1- DO YOU FEEL YOU AND YOUR FELLOW EMPLOYEES ARE NOT WELL-PREPARED TO RESPOND TO SYSTEM CRASHES IN A REMOTE WORK ENVIRONMENT?	77
FIGURE 24 PRESENTATION OF DATA FOR ENTIRE QUESTION 1- HAVE YOU FREQUENTLY ENCOUNTERED OR HEARD ABOUT MALICIOUS ACTIVITIES (E.G., PHISHING, MALWARE) WHILE WORKING REMOTELY?.....	78
FIGURE 25 PRESENTATION OF DATA FOR ENTIRE QUESTION 1- AREN'T YOU CONFIDENT IN THE COMPANY'S ABILITY TO PREVENT OR ADDRESS MALICIOUS ACTIVITIES DURING REMOTE WORK?.....	79
FIGURE 26 PRESENTATION OF DATA FOR ENTIRE QUESTION 1- DO YOU BELIEVE MALICIOUS ACTIVITIES COULD LIKELY LEAD TO SECURITY ISSUES IN A REMOTE WORK ENVIRONMENT?	80
FIGURE 27 PRESENTATION OF DATA FOR ENTIRE QUESTION 1- DO YOU FEEL YOU AND YOUR FELLOW EMPLOYEES ARE NOT WELL-TRAINED TO IDENTIFY AND AVOID MALICIOUS ACTIVITIES IN A REMOTE WORK ENVIRONMENT?.....	81
FIGURE 28 PRESENTATION OF DATA FOR ENTIRE QUESTION 1- OVERALL, HOW DISSATISFIED ARE YOU WITH THE LEVEL OF SECURITY ISSUES ASSOCIATED WITH REMOTE WORK AT LIONS RESTORATION COMPANY.....	82

List of Tables

TABLE 1 DESCRIPTIVE STATISTICS FOR ENTIRE COMPANY-SENSITIVE DATA EXPOSURE	83
TABLE 2 DESCRIPTIVE STATISTICS FOR ENTIRE EMPLOYEE-SENSITIVE DATA EXPOSURE.....	84
TABLE 3 DESCRIPTIVE STATISTICS FOR ENTIRE SYSTEMS CRASHING ISSUES	85
TABLE 4 DESCRIPTIVE STATISTICS FOR ENTIRE MALICIOUS ISSUES.....	86
TABLE 5 DESCRIPTIVE STATISTICS FOR ENTIRE SECURITY ISSUES OF REMOTE WORKING AT LIONS RESTORATION COMPANY	87
TABLE 6 CORRELATION ANALYSIS.....	88

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION - SECURITY ISSUES CAUSED BY REMOTE WORKING AT LIONS RESTORATION	17
1.1 INTRODUCTION TO LIONS RESTORATION COMPANY	17
1.2 INTRODUCTION TO SECURITY IN REMOTE WORKING	19
1.3 PROBLEM STATEMENT	25
1.4 SIGNIFICANCE OF THE RESEARCH	30
1.4.1 <i>The importance of the research to the "Company"</i>	30
1.4.2 <i>The importance of the research to the "Industry"</i>	31
1.4.3 <i>The importance of the research to "Australian Business Domain"</i>	32
1.4.4 <i>The importance of the research to "World E-Commerce Business Domain"</i>	33
1.5 RESEARCH OBJECTIVES	35
1.6 RESEARCH QUESTIONS	35
1.7 CONCEPTUAL FRAMEWORK	36
1.8 RESEARCH HYPOTHESIS	37
CHAPTER 2: LITERATURE REVIEW	38
2.1 LITERATURE REVIEW FOR COMPANY-SENSITIVE DATA EXPOSURE	38
2.2 LITERATURE REVIEW FOR EMPLOYEE-SENSITIVE DATA EXPOSURE	40
2.3 LITERATURE REVIEW FOR SYSTEMS CRASHING ISSUES	42
2.4 LITERATURE REVIEW FOR MALICIOUS ISSUES	44
2.5 LITERATURE REVIEW FOR SECURITY ISSUES CAUSED BY REMOTE WORKING AT COMPANY	46
CHAPTER 3: METHODOLOGY	48
3.1 RESEARCH UNION	48
3.1.2 <i>Research Onion Overview</i>	48
3.1.2 <i>Research Onion Layers</i>	49
3.2 RESEARCH PHILOSOPHY - POSITIVISM	51
3.2.1 <i>The chosen Research Philosophy</i>	51
3.2.2 <i>The reason for choosing Positivism of Research Philosophy</i>	51
3.3 RESEARCH APPROACH - DEDUCTIVE	52
3.3.1 <i>The chosen Research Approach</i>	52
3.3.2 <i>The reason for choosing Deductive of Research Approach</i>	53
3.4 RESEARCH CHOICE – MONO METHOD QUANTITATIVE	55
3.4.1 <i>The chosen Research Choice</i>	55
3.4.2 <i>The reason for choosing Mono Method Quantitative of Research Choice</i>	55
3.5 RESEARCH STRATEGY – MONO METHOD QUESTIONNAIRE	56
3.5.1 <i>The chosen Research Strategy</i>	56
3.5.2 <i>The reason for choosing Mono Method Questionnaire of Research Strategy</i>	57
3.6 TIME HORIZON – CROSS SECTIONAL	58
3.6.1 <i>The chosen Time Horizon</i>	58
3.6.2 <i>The reason for choosing Cross Sectional of Time Horizon</i>	58
3.7 TECHNIQUES AND PROCEDURES	59
3.7.1 <i>Target Population</i>	59
3.7.2 <i>Sample Population</i>	60

3.7.3 Data collection Method.....	60
3.7.4 The reason for choosing online-based method as Data collection Method.....	61
3.7.5 Data Analysis.....	62
3.8 RESEARCH LIMITATION.....	62
3.9 RESEARCH ETHICS	63
3.10 ACCURACY AND VALIDITY OF THE RESEARCH.....	64
CHAPTER 4: ANALYSIS.....	66
4.1 PRESENTATION OF DATA	66
4.1.1 Presentation of Data for Entire Company-Sensitive Data Exposure.....	66
4.1.2 Presentation of Data for Entire Employee-Sensitive Data Exposure	70
4.1.3 Presentation of Data for Entire Systems Crashing Issues.....	74
4.1.4 Presentation of Data for Entire Malicious Issues	78
4.1.5 Presentation of Data for Entire Security Issues of Remote Working at Lions Restoration Company	82
4.2 DESCRIPTIVE STATISTICS	83
4.2.1 Descriptive Statistics for Entire Company-Sensitive Data Exposure.....	83
4.2.2 Descriptive Statistics for Entire Employee-Sensitive Data Exposure	84
4.2.3 Descriptive Statistics for Entire Systems Crashing Issues	85
4.2.4 Descriptive Statistics for Entire Malicious Issues.....	86
4.2.5 Descriptive Statistics for Entire Security Issues of Remote Working at Lions Restoration Company	87
4.3 CORRELATION ANALYSIS.....	88
4.4 REGRESSION ANALYSIS.....	89
4.4.1 Regression Analysis for Entire Company-Sensitive Data Exposure and Security Issues of Remote Working at Lions Restoration Company.....	89
4.4.2 Regression Analysis for Entire Employee-Sensitive Data Exposure and Security Issues of Remote Working at Lions Restoration Company.....	90
4.4.3 Regression Analysis for Entire Systems Crashing Issues and Security Issues of Remote Working at Lions Restoration Company	91
4.4.4 Regression Analysis for Entire Malicious Issues and Security Issues of Remote Working at Lions Restoration Company.....	92
CHAPTER 5: CONCLUSION	93
4.5 CONCLUSION.....	93
4.5.1 Conclusion on Company-Sensitive Data Exposure.....	94
4.5.2 Conclusion on Employee-Sensitive Data Exposure	95
4.5.3 Conclusion on Systems Crashing Issues.....	96
4.5.4 Conclusion on Malicious Issues	97
4.5.5 Conclusion on Security Issues of Remote Working at Lions Restoration Company.....	98
4.5.6 Conclusion on Company-Sensitive Data Exposure and Security Issues of Remote Working at Lions Restoration Company.....	99
4.5.7 Conclusion on Employee-Sensitive Data Exposure and Security Issues of Remote Working at Lions Restoration Company.....	101
4.5.8 Conclusion on Systems Crashing Issues and Security Issues of Remote Working at Lions Restoration Company.....	103
4.5.9 Conclusion on Malicious Issues and Security Issues of Remote Working at Lions Restoration Company.....	105
CHAPTER 6: RECOMMENDATION	107
6.1 RECOMMENDATION FOR COMPANY-SENSITIVE DATA EXPOSURE	107

6.2 RECOMMENDATION FOR EMPLOYEE-SENSITIVE DATA EXPOSURE.....	109
6.3 RECOMMENDATION FOR SYSTEMS CRASHING ISSUES	111
6.4 RECOMMENDATION FOR MALICIOUS ISSUES.....	113
REFERENCES.....	115
APPENDIX 1 – TIME SCALE AND GANTT CHART.....	115
APPENDIX 2 – QUESTIONNAIRE	116
APPENDIX 2 – APPROVAL LETTER.....	119
LIST OF REFERENCES.....	120

Chapter 1: Introduction - Security issues caused by Remote Working at Lions Restoration

1.1 Introduction to Lions Restoration Company

Lions Restoration is a company based in Australia. This company uses cutting-edge technology to provide high-quality restoration services. This company's technicians are all IICRC-certified and well-trained. This company is a member of the Restoration Industry Association (RIA) as well as a certified business by the Institute of Inspection Cleaning and Restoration Certification (IICRC). The services of this business are available throughout the metropolitan area of Melbourne as well as in regional Victoria, Tasmania, and Western Australia.

This company offers a range of services including water damage restoration, carpet and upholstery cleaning, flooring solutions, odor elimination, and fire and smoke restoration. They provide high-quality services and employ advanced techniques to ensure effective and efficient results for their clients.

Lions Restoration Services' vision is to provide restoration solutions to clients quickly and collaboratively using innovative technologies and cutting-edge equipment. Through expertise and diligence, their primary objective is to satisfy customers.



Figure 1 Lions Restoration Company

Despite the Lions Restoration company being a company that operates in the field (in Australia), they need to create reports and do invoices which require office skills. Hence, they needed an administrative team to handle these documents. So, they have opened an administrative branch in Sri Lanka. But due to the COVID-19 pandemic situation, they needed a workforce which can operate at home. So, they opened a new branch in Sri Lanka at the beginning of 2022. This company is just getting into the remote working culture. They have never used it before, so they had to face a lot of technical difficulties.

While it is clear that remote work is becoming more and more popular and offers certain clear and established advantages in the modern workplace, There were several difficulties that Lions Restoration staff had to overcome as part of the changeover.

To begin with, not every company is a good fit for remote employment. For example, this Lions Restoration company requires physical work or direct client contact. Even for these companies, there is a need to adapt and get beyond obstacles to managing a highly effective remote crew to handle office work and handle projects.

When Lion Restoration company transitioned their operations online, they faced several challenges. One of the difficulties was maintaining the enriching in-person interactions that they had previously relied on to build strong relationships with their clients. They also had to prioritize IT security to ensure the safety of their online platforms and data. Leveraging online platforms for communication and collaboration became essential, as did providing active dialogue and consistent feedback to keep the team engaged and motivated. Hosting daily video calls became a regular practice to maintain communication and connection among team members. Additionally, they expanded their workforce by hiring remote workers from Sri Lanka, which required establishing effective communication channels and scheduling regular meetings, hangouts, and check-ins. Creating a collaborative online community culture was crucial to foster teamwork and cooperation, while implementing a central communication channel helped streamline information sharing. Finally, scheduling collaborative work hours ensured that team members could work together effectively despite being in different locations.

1.2 Introduction to Security in Remote Working

The act of an employee working remotely, away from the employer's main office, is known as remote work. A worker's home, a co-working space, another communal area, a private office, or any other site other than the typical corporate office building or campus could be considered such places. Because it has advantages for both businesses and employees, remote work has grown in popularity. The COVID-19 epidemic, which compelled many businesses to swiftly transition from a conventional face-to-face work environment to a completely remote workforce for health and safety reasons, also significantly renewed interest in it.

However, with borderless teams transcending the boundaries of cities, states and often continents, Lions Restoration also have a ton of sensitive data moving outside the confines of the office and across a myriad of devices, often with questionable security arrangements. To completely realize the benefits of working with the finest minds regardless of their geographical limits, Lions Restoration must understand and manage the difficulties associated with a mobile workforce. Even large corporations with multimillion-dollar budgets struggle to manage remote staff. The difficulty is greater for small businesses that must operate with limited funds and a low risk of vulnerabilities. Lions Restoration company must carefully consider the technology and security they use when working with remote staff.

As Lions Restoration company embraced a borderless workforce, they faced several critical data security issues that needed to be addressed. One concern was the reduced security on Bring Your Own Device (BYOD) and mobile devices, as these devices may not have the same level of protection as company-owned devices. Tracking and managing assets on the cloud became crucial to ensure data integrity and prevent unauthorized access. Implementing adequate backup and recovery systems was necessary to safeguard data in case of any unforeseen incidents. Compliance with the General Data Protection Regulation (GDPR) was a priority to protect the privacy and rights of individuals. Sensitizing remote teams about data security protocols was vital to ensure consistent adherence to security measures. Additionally, the company had to be vigilant about potential attacks on remote-

working infrastructure and address the risk of malicious insiders or housemates who may have access to sensitive information.

(Dholakiya, 2022)

Our business may be more severely harmed by the careless or malicious conduct of those who have authorized access to our systems than by the actions of external attackers. According to the 2022 Cost of Insider Threats Global Report by the Ponemon Institute, the average cost of a single insider threat occurrence will be between \$484,931 and \$804,997.

The good thing is that by studying examples of security mishaps from other businesses, we can prevent falling prey to security threats. The organizations listed below are some well-known ones that have lately experienced security incidents.



Renowned Organizations That Recently Suffered Security Incidents		
 Twitter	 Ubiquiti Networks	 International Committee of the Red Cross
 Shopify	 Cash App	 Intel
 proofpoint	 Pfizer	 VOLKSWAGEN <small>AKTIENGESELLSCHAFT</small>

Figure 2 some well-known businesses that have lately experienced security incidents

Phishing attack on Twitter:

We can start by examining the Phishing assault that the Twitter company experienced. Phishing is at fault for more than 60% of social engineering-related occurrences, according to the 2022 Verizon Data Breach Investigations Report. Additionally, along with downloaders and ransomware, phishing is one of the top three methods used by malicious attackers to cause breaches.

Hackers who pretended to be from the company's IT department contacted several of Twitter's remote employees and requested their login information. The attackers used these credentials to access the social network's administrator tools, reset the Twitter accounts of several prominent people, and broadcast fraudulent messages.

We can learn from this that setting up a cybersecurity policy with detailed guidelines is crucial, but it might not be sufficient. Organizations should also regularly train their staff to ensure that they are completely aware of the main guidelines of that policy and to raise their level of cybersecurity awareness. Company employees will be less likely to fall for scammers' traps if they are aware of who, how, and under what conditions they can reset their passwords. Since users of privileged accounts frequently have access to the most important systems and data, they need extra security. The consequences for an organization's security and reputation might be catastrophic if hackers acquire access to such accounts. Businesses can consider implementing systems that allow for continuous user monitoring, Multi-Factor Authentication (MFA), and User and Entity Behavior Analytics (UEBA) to guarantee the prompt detection and prevention of criminal activity under privileged accounts.

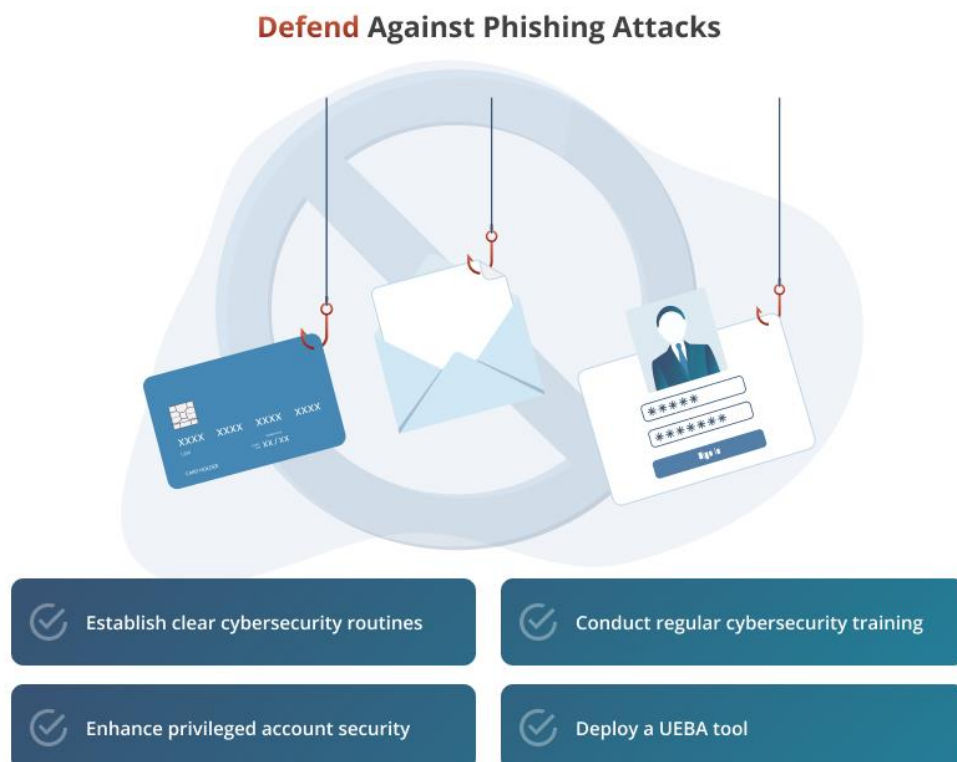


Figure 3 Ways to defend against phishing attacks

Insider data theft on Shopify and Cash App Investing:

The well-known e-commerce platform Shopify suffered an insider attack in 2020. Nearly 200 online retailers' transaction records were stolen by two Shopify workers for a fee. The hired cybercriminal received screenshots and Google Drive links with client data from malicious insiders. In the company's announcement, basic contact information and order details for customers of hacked merchants may have been disclosed. Due to the attackers' lack of access, Shopify states that no sensitive financial or personal information was impacted by the incident.

Block, Inc. disclosed a cybersecurity problem that happened in its subsidiary company Cash App in December 2021. Internal reports containing details on more than 8 million previous and present Cash App Investing users were downloaded by a former employee. The business stated that the stolen reports did not contain any personally identifiable information, such as usernames, passwords, or Social Security Numbers, but made no mention of why or how long the former employee continued to have access to private internal information.

What we can learn from this is, Limiting users' access to sensitive data is the first step in securing an organization's data. To build reliable access management and safeguard crucial systems and priceless data from potential compromise, organizations can think about putting the least privilege concept into practice. Furthermore, user activity monitoring and audits can assist the cybersecurity team in detecting questionable behaviour by employees, such as accessing data or services unrelated to the role, accessing public cloud storage services, or sending emails with attachments to personal accounts. When an employee's contract expires, companies should make ensure that an appropriate off-boarding procedure is followed. Deactivating accounts, VPN access, and remote desktop access, altering access codes and passwords the employee may know and removing the employee's accounts from email groups and distribution lists should all be included.

Prevent Insider Data Theft



Figure 4 Ways to prevent insider data theft

Third-party vendor attacks on Volkswagen:

Volkswagen announced in May 2021 that criminal actors accessed an unsecured sensitive data file by hacking a provider with which Volkswagen dealers collaborated for digital sales and marketing. Over 3 million existing and future Audi customers were affected by the incident. While the majority of the compromised data contained merely customers' contact information and information on the vehicle purchased or inquired about, around 90,000 consumers' sensitive data was also exposed. Volkswagen, in turn, guaranteed free credit protection services to individuals affected.

We can learn from this that when selecting a third-party vendor, they must consider their cybersecurity practices and compliance with rules. If a possible subcontractor lacks key critical cybersecurity practices for the firm, consider including a comparable condition in the service-level agreement. Furthermore, a firm could restrict a subcontractor's access to vital data and systems to the degree required for their job. Apply extra cybersecurity measures like MFA, manual login approvals, and just-in-time privileged access management to improve the protection of most essential assets. Also, firms can consider

using monitoring tools to track what is being done with their important data. Keeping track of third-party user activity permits quick and thorough incident investigations and cybersecurity audits.



Figure 5 Ways to prevent third party vendor attacks

Attackers are responsible for a wide range of security issues, including sensitive data leakage and breaches, trade secrets and insider data leaks, authority misuse, and phishing attempts. Analyzing the most recent examples of security breaches in other firms might assist us in identifying security weaknesses in our corporate network as well as flaws in our cybersecurity policy. After hearing about other people's experiences, we may want to reevaluate our organization's data protection policy to make it more effective against malicious threats.

(EKARAN, 2022)

1.3 Problem Statement

The main cause behind continuing this research was the number of security concerns around remote working at the Lions Restoration organization. Mrs Madhee Abeyratne, the head of the administrative department, provided me with the chance to speak with Dushmantha Randeniya, the IT lead there, during our conversation.

The biggest concern they faced with Remote Working was that employees were accessing company data using unprotected internet networks. The reason for this is that when Lion Restoration Company launched the Remote Working environment in Sri Lanka, the first thing they did was provide computers, routers and monitor displays for their employees to work. The company's management seemed less concerned about security problems back then. Many employees who worked remotely used unsecured home wireless networks or the open Internet to access their employer's data. That was opening the door for hackers to access sensitive and private information, intercept communications, and steal the information. This was discovered when management performed an employee survey, the results of which are displayed below along with the survey question.



Figure 6 Survey result for question 8

When working from home, 67 % admitted to moving data between their personal computers and their workplace PCs, which is a concerning behavior. Because HR didn't have enough funding to provide personal computers or routers for employees to use at work, some employees were permitted to use their own personal computers. Employees may then store private information on their computers without any security measures in place, which poses a threat. A security breach may occur if that employee leaves the company or if the device doesn't have the most recent security software installed. The company data sheet below shows the number of employees hired annually with and without supplying company-issued remote working tools such as company computers, office routers, and other accessories. I may conclude from this that the company didn't give much thought to this security issue, which is why they employed a large number of employees without giving them company resources to use for work-related tasks. The graph below shows the number of employees recruited each year with or without remote working equipment by the company.

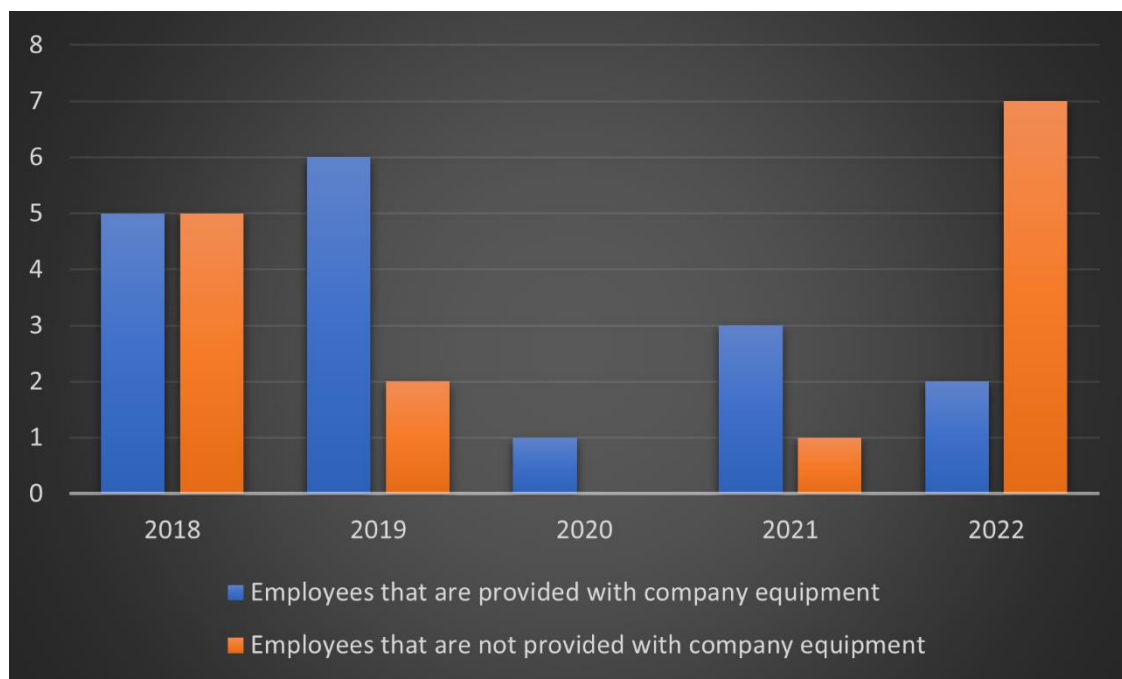


Figure 7 The number of employees recruited each year with or without remote working equipment by the company

During this research, I spoke with a few employees and noticed that they didn't follow fundamental security practices when speaking with outsiders. Some of them were working for the company when I met them, but I could see what they were doing, and they didn't

even seem to mind that I was looking at their screens. When it comes to sensitive information belonging to the firm, we cannot entirely ignore physical security. There could be workers who, for instance, talk loudly on the phone when in public, display their laptop screen for everyone to see inside a café, or even leave their equipment unattended. These observations, therefore, caught my attention, and I believed I should consider this as well when conducting my research. It can be challenging for smaller companies such as Lions Restoration company to prioritize data loss prevention, backup, and recovery since they have a long list of more pressing issues to solve. However, neglecting the problem for an extended period of time might be dangerous.

Another concern that I noticed was that some remote workers were using the same device for both personal and professional purposes. They frequently seemed to mix together personal and professional information, leaving both vulnerable. Therefore, if a worker's laptop fails as a result of a malicious file downloaded for personal use (such as a pirated game or movie), the company data also is destroyed. If they are exposed to such a threat or attack, recovering this data may become difficult or impossible. Under the supervision of Lions Restoration company management, I was able to obtain a screenshot of a previous employee's laptop, and I was forced to blur company-related files and web applications for their own protection. The below figure represents that screenshot. According to the figure, personal files of past employees can be found among the Lion Restoration company's files and applications.

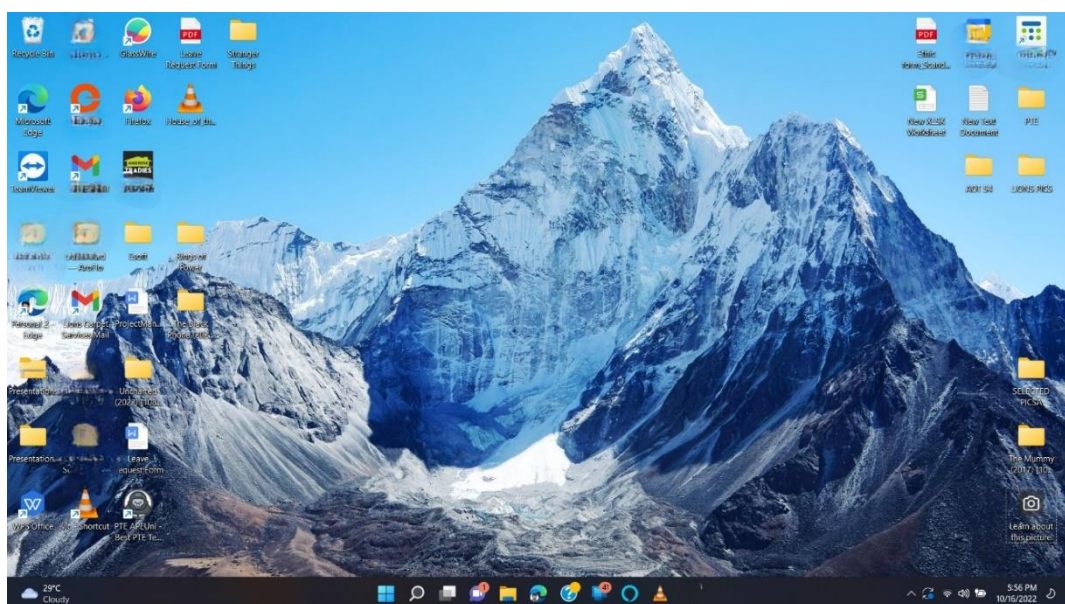


Figure 8 Past employee desktop screen shot with having company and personal data mixed up

The system analyst said that they discovered some employees using their corporate email for both personal and unauthorized web sites. So, the company management conducted an investigation of all of the employees' emails under the corporate domain and discovered that the number of employees who used their email for unapproved websites grew by 30% this year as given figure below.

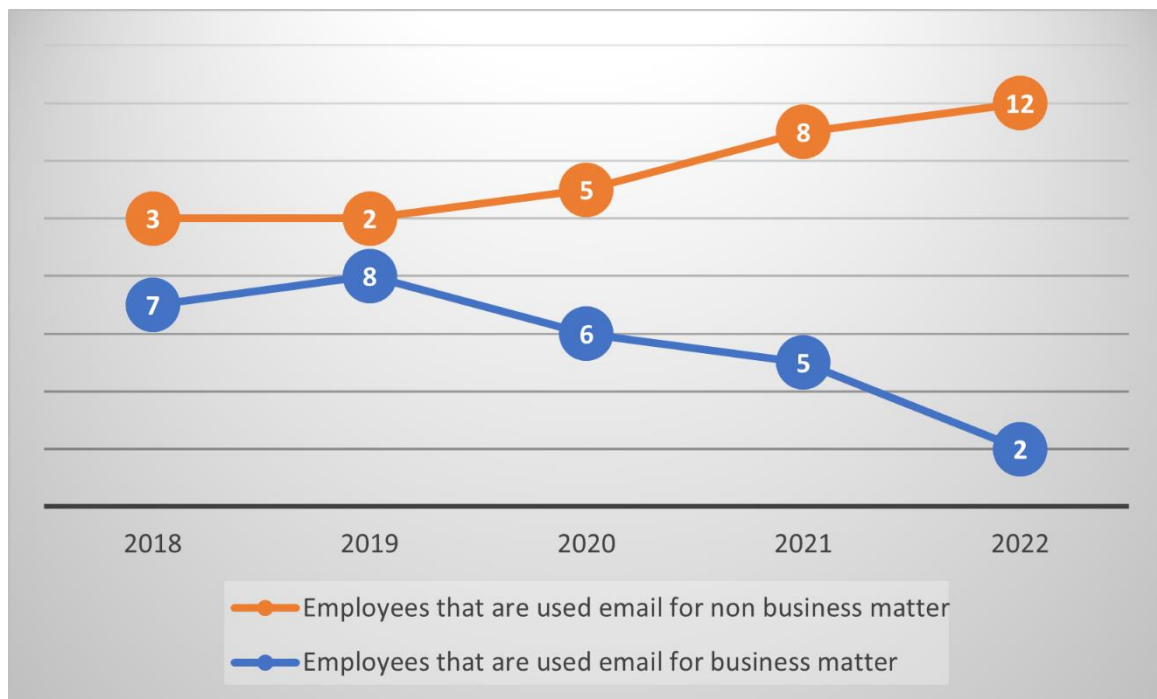


Figure 9 Number of employees used their corporate email for unauthorized web sites and not

Employees all over the world are victims of phishing or email scams that are getting more and more advanced. Lions Restoration company remote working Employees may send emails that seem trustworthy and authentic, but by responding or clicking on links, they may be tricked into supplying sensitive information, bank information, or even sending substantial amounts of money into the wrong bank account. Or harmful viruses may invade company files, erasing all of the company data and disrupting business operations.

Finally, the HR management gave me a detail of the money they spent on equipment repairs and maintenance for remote workers, as seen in the figure below. According to these cost sheets, the prices of repairing physical and software damages to employee remote working devices have gradually increased. As a result, some employees may attempt to repair the equipment by studying internet tutorials, and they may download harmful software to do

so. Before things got out of hand, I was concerned about this and incorporated it in my research to discover the best potential solutions for them.

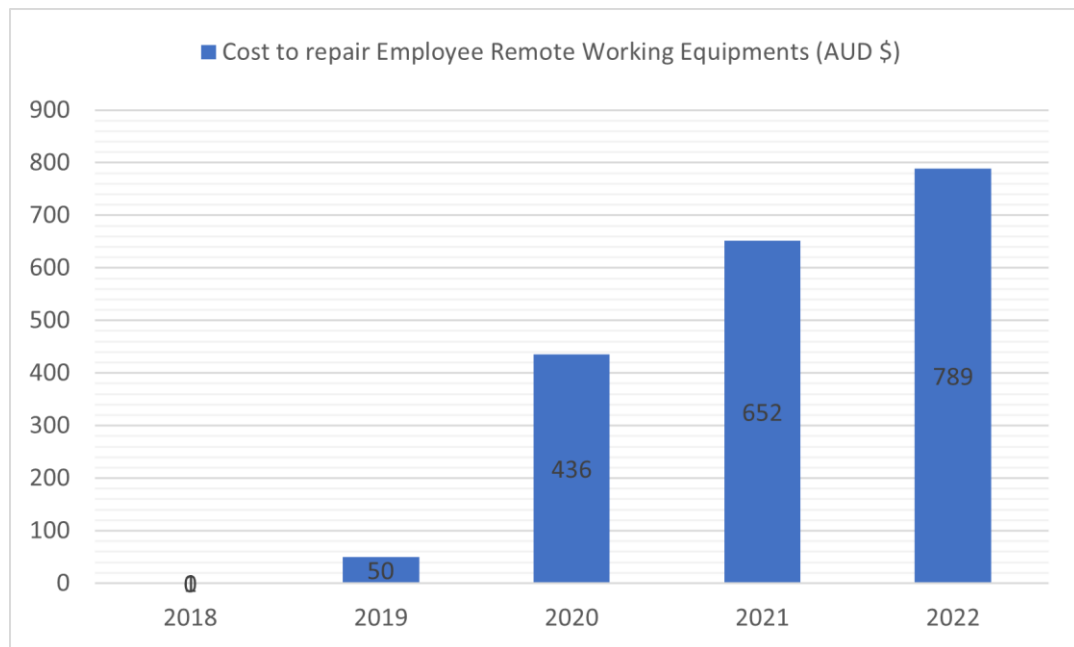


Figure 10 Cost sheet on equipment repairs and maintenance for remote workers

As a result of their lack of security worries for their work and equipment, the remote working team has unintentionally put the company in danger. The pandemic forced the company into a quick digital transformation, and as a result, cybersecurity has grown to be a key problem. When the COVID-19 outbreak started and employees had to start working remotely, this business was unprepared in terms of security issues. Employees that operate remotely could unwittingly compromise the security of the entire business. Many employees lacked the necessary training, skills, and understanding to safeguard their equipment against cyber-attacks. That is why it is critical that this company supports and capacitates its employees in identifying threats, knowing what to do if they suspect a breach, and assisting them in obtaining the appropriate security software and gear to prevent cyber-attacks.

1.4 Significance of the Research

1.4.1 The importance of the research to the “Company”

Since nobody wants to lose their possessions, security is a must for all businesses. The news that our business has been damaged into by intruder and valuable items and equipment have been stolen is the most terrible thing anyone can hear. The development of our business is halted, and recovering the losses uses up a large percentage of our resources. If we don't establish a security system in our company, we are putting the security of our entire operation in danger.

So, because no one has undertaken a study on Security Issues in Remote Working in this Lions Restoration company, this is a better opportunity to uncover faults in security concerns in remote working in the business. They just used general security procedures, such as regular password approaches, to access the system. So this was a fantastic opportunity for the Lions Restoration company to discover their security issues in remote working.

This organization has encountered security difficulties while remote working and those issues have gradually increased over time. Once, a newly hired university employee of the company unintentionally exploited cooperative email to subscribe to several websites and channels, and the issue was discussed with the management. However, in my opinion, the precautions they adopted after that were insufficient. As a result, this research serves as a tool for assessing the company's security concerns in remote working in order to secure the company's and every asset. This study investigates the risks that the company faces in remote working and the weaknesses that it has, as well as the safeguards in place to reduce responsibility. We can discover vulnerabilities and make fixes before or after an incident or loss occurs.

After the COVID outbreak, this corporation has restricted remote working staff. As a result, the risks of having security issues occur in remote working are reduced, but there is a significant likelihood that this work-from-home culture will be widely implemented in this organization in the near future. Because the management is interested in reintroducing the work-from-home culture to the business because it can generate significant money. As a

result, this is an excellent opportunity for them to take appropriate measures before broadening their work-from-home culture in the business again. So there are serious security weaknesses in the company's remote working culture, as I mentioned in the problem statement. Additionally, there is a history of security difficulties with remote working at this organization. As a result, this research will assist this company in identifying and comprehending precisely what needs to be safeguarded in their remote working systems and the necessary procedures.

1.4.2 The importance of the research to the “Industry”

Lions Restoration is a forerunner in the Australian restoration industry. However, there are several restoration companies in Australia that conduct large operations, as Lions Restoration does. As a result of the pandemic, many businesses had to shift remote working cultures in order to continue administrative operations. So, this is not an issue that the Lions Restoration company has solely encountered. Every other restoration company in the field had to deal with the same issue. So, I believe this research would be beneficial to those businesses as well because there were no research publications on this subject on the internet.

I conducted this research on the Lions Restoration company, which will assist not only the company but also the restoration industry. However, this research is useful for any administrative industry in any field. Administrative employment in banking, finance, construction, education, or any other distant worker as an administrator can benefit from this research.

Administrative personnel that work from home in the restoration sector must log into various cooperating sites using different login passwords. And in this industry, technicians who work in the field uploading data and information from sites to those systems can access them from anywhere in the world if they have the proper login credentials. Unfortunately, the hired employees in this profession are regular people. Most of them do not have extensive IT knowledge or experience in cyber security. As a result, in this industry, most

businesses are extremely vulnerable to cyber-attacks. Knowing potential issues in remote working is essential if organizations want to be in business for a long time.

And also, any remote administrative assistant, also known as a “virtual assistant”, who may have a variety of responsibilities, such as making phone calls, typing and reviewing documents, gathering data, updating blogs and social media, making travel arrangements for management teams, preparing presentations, and assembling reports, can benefit from this research. So that they can address any challenges that may occur or have arisen as a result of this research. So, this research is valuable to numerous industries, and they may move forward with confidence in the global market if this research is followed up on.

1.4.3 The importance of the research to “Australian Business Domain”

Australian E-Commerce Business Domain cyber security problems are still escalating at a startling rate. Eight out of ten Australian E-Commerce Business Domain use the internet every day, increasing the danger of online crime, stolen data, and exploitation. Given that the national cost of cybercrime is estimated to exceed \$1 billion yearly, it is crucial for the Australian government to create a robust IT security industry that enables people and businesses to do business online in a secure manner. However, despite being industry leaders, the majority of organizations do not implement adequate cyber security measures because significant attacks have not yet occurred. Therefore, not just in the administrative industry is this a serious problem. The entire nation is affected by these security concerns with remote working.

It's interesting to note that 64% of Australian E-Commerce Business Domain private sector businesses want to implement these top remote work practices. All Australian E-Commerce Business Domain businesses must take precautions to lessen their vulnerability to cyberattacks, which are growing more sophisticated. Cybersecurity incidents are also on the rise, according to the Australian Cyber Security Centre (ACSC).

These security risks are a threat to Australia's economic well-being and national interests since they are becoming more frequent, larger, and more sophisticated. In order to save

costs and improve security in all enterprises around the country, the Australian government can even take into consideration the research I've done.

With the COVID pandemic, the majority of Australian E-Commerce Business Domain firms embraced remote working in their businesses. Therefore, there is a high possibility that they would require this kind of research to eliminate security issues as they expanded their businesses. And also due to the number of studies conducted on security threats in remote working in Australian E-Commerce Business Domain businesses is negligible. However, this study demonstrated all the significant security concerns that could arise from remote work as well as feasible strategies to address them. Due to the fact that this research took into account all of the environmental variables affecting Australian firms, both the government and industry will benefit significantly from it.

1.4.4 The importance of the research to “World E-Commerce Business Domain”

Working from home has grown considerably more popular since the pandemic. Analysts predict that remote working will continue to be widespread across many industries even after the pandemic has passed. While having the ability to work from home is efficient and has many advantages, it also exposes people and businesses to a number of security threats. That is why it is critical to take home cybersecurity seriously.

Because of the increase in remote work, phishing and other security concerns have grown in frequency. In the majority of companies, an IT staff will handle office security. However, with a scattered workforce working remotely, employees must give more importance to cybersecurity issues. Unfortunately, the majority of people who work from home are unaware of the security implications of remote work, and very few know how to apply basic security practices. Therefore, all businesses across the world can use this research to strengthen the security of their remote working operations and to educate their staff.

There are many risks associated with having employees work remotely because they frequently use their personal devices and home networks to execute tasks. 70% of remote workers reported having IT issues during the pandemic, and 54% reported having to wait up to three hours for a solution, according to the Velocity Smart Technology Market

Research Report 2021. Furthermore, according to a Gartner survey, 47% of organizations will allow employees to work remotely full-time once the epidemic is over, and 82% stated employees could work from home at least one day per week.

Organizations are having difficulty controlling the use of mobile devices by remote workers, according to the CISO's Benchmark Report 2020. Many employees use personal devices to perform two-factor authentication. And employees may also use mobile apps like Teams and Zoom to communicate with people all around the world. The possibility of sensitive information entering an unsecured environment grows as a result of these blurred boundaries between professional and personal life. The IT team is having huge headaches because there is nothing, they can do to safeguard employees from this. Indeed, 52% of respondents in CISCO's report stated that mobile devices pose a serious risk to cyber security.

So, before doing this research, I was aware of all the possible environments that influence remote working culture. This study can be used by any businesses across the world that use remote working to protect their firm networks and personnel. Because every company has an administration team that handles all of the reports, records, finances, and projects. So that enterprises can acquire the trust of their clients, they may confidently extend their businesses around the world if they undergo proper research in this manner. As a result of this research, businesses, and governments everywhere in the world can simply mitigate most cybersecurity threats when working from home. This research covers all of the major areas of security issues in remote working, as well as this, has given possible solutions so that all businesses throughout the world can lessen their vulnerabilities to potential threats by following this research.

1.5 Research Objectives

Objective 1 : To find out whether remote working cause company sensitive data exposure at Lions Restoration Company.

Objective 2 : To find out whether remote working cause employee-sensitive data exposure at Lions Restoration Company.

Objective 3 : To find out whether remote working cause company systems crashing issues at Lions Restoration Company.

Objective 4 : To find out whether remote working cause malicious issues at Lions Restoration Company.

1.6 Research Questions

Research Question 1 : Is company sensitive data exposure caused by remote working at Lions Restoration Company?

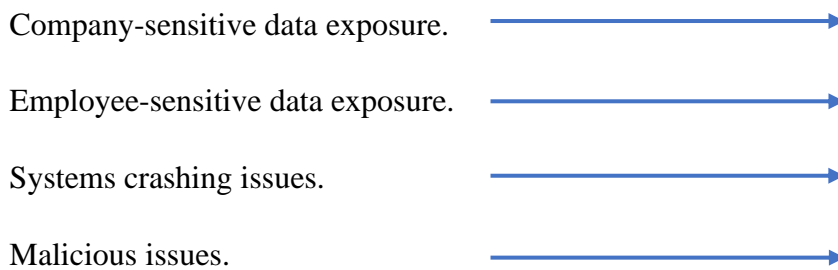
Research Question 2 : Is employee-sensitive data exposure caused by remote working at Lions Restoration Company?

Research Question 3: Are company systems crashes caused by remote working at Lions Restoration Company?

Research Question 4: Are malicious issues caused by remote working at Lions Restoration Company?

1.7 Conceptual Framework

Independent Variables



Dependent Variable

Security issues of remote working at
Lions Restoration Company.

1.8 Research Hypothesis

Research Hypothesis for company sensitive data exposure and security issues of remote working at Lions Restoration Company.

H0: Company sensitive data exposure is not caused by remote working at Lions Restoration Company.

H1: Company sensitive data exposure is caused by remote working at Lions Restoration Company

Research Hypothesis for employee-sensitive data exposure and security issues of remote working at Lions Restoration Company.

H0: Employee-sensitive data exposure is not caused by remote working at Lions Restoration Company

H1: Employee-sensitive data exposure is caused by remote working at Lions Restoration Company

Research Hypothesis for systems crashing issues and security issues of remote working at Lions Restoration Company.

H0: Systems crashing issues are not caused by remote working at Lions Restoration Company

H1: Systems crashing issues are caused by remote working at Lions Restoration Company

Research Hypothesis for malicious issues and security issues of remote working at Lions Restoration Company.

H0: Malicious issues are not caused by remote working at Lions Restoration Company

H1: Malicious issues are caused by remote working at Lions Restoration Company

Chapter 2: Literature Review

2.1 Literature Review for Company-Sensitive Data Exposure

Since the cost of a data breach rises year after year, it has become a major issue for enterprises. According to a RiskRecon, 2018 survey, sponsored by Mastercard and performed by Ponemon Institute, just 34% of respondents believe a major third party will inform their partners of a data breach. In addition, 43% of respondents stated that their organizations regularly examine their third-party management policies and practices. More than half of respondents also stated that they depended on the third party to inform their organization whenever data was shared with Nth parties. A data breach could happen in any industry that gathers, stores, or processes sensitive data. According to estimates for both direct and indirect costs, the average cost of a data breach in 2020 will be \$3.86 million to contain. Companies may be at risk of a significant breach if they have inadequate security, are unable to comply with legislation, identify vulnerabilities, and provide adequate data protection (Mirza, 2020). A data breach can harm an organization's reputation by costing money in fines, court costs, and losing customer trust.

3 billion user accounts were affected by the largest case of sensitive data exposure to date. Hackers collected 1 billion user credentials, including email addresses, passwords, and security questions and answers, as a result of the 2013 Yahoo! data breach. In 2014, Yahoo! was the victim of new hackers who affected 500 million users. Three years after the initial hack, in 2016, both incidents were finally made public. In the end, 3 billion accounts were compromised, customer confidence plummeted, and the company's value was reduced by millions (Dan Swinhoe et al, 2021)

In 2017, a breach occurred at Equifax, the top provider of credit reports in the US. Hackers who discovered a server vulnerability and an expired encryption certificate were able to

steal millions of user credentials and personal information (PII). Hackers who gained access to the Equifax system were able to take plain-text copies of user credentials and use them to log into both administrator and user accounts. Attackers sent HTTP requests containing malicious code by utilizing Java's open-source network to their advantage. These malicious executions were successful, exceeding authorizations and maintaining access for almost two months without any indication of suspicious behavior. Due to their failure to reveal the breach for more than a month after it was initially detected, Equifax suffered severe reputational damage (Mirza, 2020)

LinkedIn experienced a breach in 2012 when it revealed that 6.5 million random passwords (SHA-1 hashes) had been taken by thieves and uploaded on a Russian hacker forum. Unfortunately, the entire scope of the incident wasn't made public until 2016. The email addresses and passwords of around 165 million LinkedIn members were discovered to be being sold by the same hacker who was selling the data from MySpace for just 5 bitcoins (approximately \$2,000 at the time). LinkedIn stated that it had changed the passwords for the impacted accounts after becoming aware of the breach (Dan Swinhoe et al., 2021).

Sensitive data disclosure is a critical risk for companies since it can have negative effects on their reputation, cause them to lose money, and put them in legal trouble. Organizations must take a number of precautions to prevent the exposure of sensitive data. In order to maintain track of all the data held within their systems and to have a clear understanding of the owners, locations, security, and governance mechanisms of that data, they must first conduct an audit (Baig, 2022). Second, they must evaluate the risks related to the data and allocate funds and resources in accordance with their findings (Baig, 2022). The more sensitive the data, the greater the chance of harm. Even a little amount of extremely sensitive data can have serious consequences for data subjects (Baig, 2022).

Thirdly, companies need to put the right security measures in place to prevent sensitive data exposures and lessen the effects they have on data subjects (Baig, 2022). In order to

respond quickly to the exposure of sensitive data, organizations must have a strong breach response system in place (Baig, 2022). The aforementioned steps can assist companies in preventing the exposure of sensitive data, but they must make sure that these steps are routinely evaluated and updated to reflect evolving security threats and data protection laws.

2.2 Literature Review for Employee-Sensitive Data Exposure

Data breaches have alarmingly increased over the past few years, and along with them, the sensitivity of the exposed data. The average cost of a data breach worldwide is \$4.24 million, according to a report by IBM (Gasparian, 2022). These data breaches frequently result from the unintentional disclosure of sensitive information, which can happen for a number of reasons.

Given the complicated IT environments that most modern businesses have adopted, it may not be all that unexpected if efforts to protect sensitive information fail. Employee mistakes and a lack of controls are potential causes (Nimrod Iny, [2022]). Threat actors directly utilize a variety of tactics, including SQL injection attacks, man-in-the-middle attacks, and social engineering attacks, to expose and access sensitive data (Nimrod Iny, [2022]).

Employee error is one of the main reasons why sensitive data gets exposed. A data breach that happened as a result of insufficient security measures, human error, or both may be referred to as a "accidental exposure" (Gasparian, 2022). The majority of security experts agree that insider threats are increasing, with employees being the primary source of data breaches (Jeremiah Talamantes, 2018). The biggest threat is seen to come from privileged employees with access to sensitive information (60%) followed closely by consultants and contractors (57%) and regular employees (51%) (Jeremiah Talamantes, 2018).

Lack of sufficient training is another risk that exposes sensitive data. All businesses must safeguard themselves and their staff from data breaches, which frequently happen when an employee opens a link in a phishing or other malicious email (Gasparian, 2022). The danger of unintentional exposure can be decreased by implementing a mandated cybersecurity training program to instruct all staff levels on phishing, social engineering, and other forms of fraud (Gasparian, 2022).

Organizations can take a number of precautions to safeguard their employees from exposure to sensitive data. Some of the suggested actions are as following. Workers can use complex and one-of-a-kind passwords. It's crucial to have different, complicated passwords for all of the internet accounts. It can be challenging to keep track of all those passwords, but there are tools available that can assist, such as Password Manager (Norton, 2021). Financial Accounts Should Be Monitored by Employees. Employees need to frequently check their bank and other financial accounts for unusual activity. It might make sense for employees to sign up for activity alerts by text or email if the companies offer them (Norton, 2021).

Credit reports should be checked by employers. To find out if a thief has attempted to open a new credit card or other account in their name, employees should routinely check their credit report. Every 12 months, they are legally entitled to a free credit report from each of the three major credit reporting agencies (Norton, 2021). Employers should receive regular training in cybersecurity. Companies ought to put in place a required cybersecurity training course to inform all staff members about phishing, social engineering, and other forms of fraud. The risk of unintentional exposure can be reduced by using particular examples to "teach" personnel how to handle these kinds of threats (Gasparian, 2022).

2.3 Literature Review for Systems Crashing Issues

The issue of systems failure is serious and can cause firms to suffer grave financial and reputational losses. Hardware malfunction is one of the key reasons why systems crash. Almost one-third of all system crashes, according to research, are caused by hardware malfunctions (Liu et al., 2017). Overheating, power surges, and component failure are only a few of the causes of these problems. Using redundancy and backup systems, as well as routinely monitoring and maintaining gear, helps reduce the effect of hardware failures (Liu et al., 2017). Software malfunctions are another frequent reason for system crashes. System crashes can be caused by software defects, coding mistakes, and conflicts with other software (Zhang et al., 2019). Software crashes can be particularly challenging to identify and resolve since they may not be immediately obvious and can be challenging to reproduce. Using strict testing and quality control techniques during the software development process is one way to address this issue (Zhang et al., 2019).

System failures can also be largely attributed to human error in addition to hardware and software issues. Up to 80% of system crashes, according to research, are the result of human mistake (Huang et al., 2017). These mistakes can be made when configuring the system, when adhering to protocols, and when accidentally deleting important files. Organizations can implement strict employee training and education programs, as well as enforcing rigorous protocols and procedures, to reduce the risk of human error (Huang et al., 2017).

System crashes are frequently caused by network problems as well. Hardware failure, software problems, and cyberattacks are just a few of the many causes of network failures (Sayed et al., 2018). Using redundancy and backup systems, as well as routinely monitoring and repairing network hardware and software, helps reduce the impact of network failures (Sayed et al., 2018). System crashes are becoming frequently caused by cyberattacks. Cyberattacks such as malware, viruses, and others can seriously harm organizational

systems, resulting in data breaches and system breakdowns (Zargar et al., 2013). Using strong cybersecurity measures, such as firewalls, antivirus software, and intrusion detection systems, can reduce the impact of cyberattacks (Zargar et al., 2013).

In addition to studying the causes of system crashes, researchers have looked into the effects of system crashes on organizations. System failures can cause considerable financial losses and reputational harm to an organization (Wang et al., 2019). By developing strong disaster recovery and business continuity plans, as well as routinely testing and upgrading these plans, the effects of system crashes can be reduced (Wang et al., 2019).

The application of artificial intelligence (AI) and machine learning (ML) technologies is one potential solution for the issue of system crashes. AI and ML can be used to analyze system data and spot potential problems before they arise in order to predict and prevent system crashes (Bhadauria et al., 2019). However, using AI and ML also has drawbacks, such as the necessity for high-quality data and the possibility of false positives (Bhadauria et al., 2019).

In conclusion, system crashes are a significant issue for companies and can be brought on by a number of things, including faulty hardware or software, human error, network problems, and cyberattacks. By developing thorough disaster recovery and business continuity strategies and routinely monitoring and maintaining hardware, software, and networks, system crashes can be reduced in severity. More study is required to fully investigate the possibilities of AI and ML technologies, which may also offer a promising option for anticipating and mitigating system crashes.

2.4 Literature Review for Malicious Issues

As enterprises face a rising number of security threats that cause data breaches, financial losses, and reputational damage, malicious assaults have emerged as a common problem in the current digital era. Any deliberate action with the intent to hurt, exploit, or breach the network or systems of an organization is referred to as a malicious attack. This can be done for vengeance or personal gain. Malicious assaults are carried out by cybercriminals using a variety of methods, including phishing, malware, ransomware, and distributed denial-of-service (DDoS) attacks.

Phishing, which involves pretending to be a reliable entity in electronic communication, is an attempt to get sensitive information by deception. A survey by Radicati Group found that 1 in 99 emails are phishing assaults, which are on the rise with 306.4 billion emails received daily (Radicati Group, 2021). Phishing attacks have advanced as a result of cybercriminals' use of social engineering techniques to prey on users' vulnerabilities and trick them into providing sensitive information. Organizations must educate staff members about phishing attacks and put in place technical safeguards like email filtering and multi-factor authentication (MFA) (Asante et al., 2019).

Any software that is intended to damage, interfere with, or seize control of a computer system is referred to as malware. Malware can enter a system through a number of channels, including email attachments, compromised websites, and portable devices. A form of virus called ransomware encrypts the victim's files and requests a ransom in return for the decryption key. Ransomware damages, which cost \$325 million in 2015, will cost the world \$20 billion by 2021, according to a report by Cybersecurity Ventures (Cybersecurity Ventures, 2021). Organizations must keep their antivirus software up to date, regularly review their vulnerabilities, and employ security controls like firewalls and intrusion

detection and prevention systems (IDPS) to lessen the effects of malware and ransomware assaults (Kshetri, 2018).

DDoS attacks include flooding a network or server with traffic in order to prevent it from operating normally. A botnet, or network of compromised devices under the attacker's control, is frequently used in DDoS attacks. DDoS attacks grew by 542% in the first quarter of 2020 compared to the same period in 2019, according to a report by Akamai Technologies (Akamai Technologies, 2020). Using network security measures like firewalls, load balancers, and content delivery networks (CDNs) help reduce the impact of DDoS attacks (Liao et al., 2018).

Cybercriminals utilize the method of social engineering to convince people to reveal sensitive information or take security-compromising acts. Pretexting, baiting, phishing, and pretexting are all types of social engineering attacks. According to a Ponemon Institute report, 56% of data breaches in 2020 will be the result of social engineering attempts (Ponemon Institute, 2021). Organizations must create access controls, train employees in security awareness, and monitor user behavior to prevent social engineering attacks (Choo et al., 2018).

In conclusion, malicious attacks pose a severe threat to the security of organizations and can have catastrophic effects. Companies must adopt a thorough security strategy that includes employee education and awareness campaigns as well as technical safeguards like firewalls and anti-virus software. In order to find and close any security gaps, companies should do frequent risk assessments and vulnerability scans. Organizations can lessen the effect of malicious attacks and the danger of a security breach by adopting a proactive security strategy.

2.5 Literature Review for Security issues caused by Remote Working at Company

Several businesses have had to adapt to this new reality as a result of the COVID-19 epidemic, which has caused an extraordinary rise in the number of people working remotely. While there are numerous advantages to working remotely, there are also security concerns that companies must address in order to safeguard critical information and prevent cyberattacks.

Employees accessing company data and systems from outside the regular security perimeter is one of the main issues with remote working. This could increase the possibility of security breaches and the risk of unauthorized access to sensitive data. Since the start of the epidemic, 45% of businesses have had a security incident involving remote work, according to a survey by IBM Security (2021).

Employees using personal networks and devices that don't have the same level of security as company-provided infrastructure presents another difficulty. As a result, it might be simpler for attackers to use insecure networks and devices access access corporate data. According to Kaspersky (2021), since the start of the epidemic, 34% of companies have reported a security incident involving a personal device.

Companies must put in place efficient security measures for remote workers to reduce these threats. One method is to link the employee's device to the workplace network securely using virtual private networks (VPNs). The Ponemon Institute (2020) found that 60% of businesses use VPNs to protect remote connections.

Giving personnel training on how to recognize and prevent security dangers, such as phishing emails and social engineering assaults, is another crucial security precaution. This can lessen the possibility that workers will unintentionally provide hackers access to

company data. A Trend Micro analysis from 2020 states that since the epidemic began, 45% of businesses have boosted their security awareness training. Companies should also think about installing multi-factor authentication (MFA) for remote access to sensitive data and systems in addition to these precautions. Even if an attacker obtains the employee's password, this can assist prevent unwanted access. From January to April 2020, MFA usage among Okta clients climbed by 13%, according to a report by Okta (2020).

Furthermore, organizations should continuously examine and update their security policies and processes to make sure they are applicable and efficient in the context of remote working. This can involve taking steps like routinely evaluating vulnerabilities, developing an incident response, and following data backup and recovery processes. According to the National Institute of Standards and Technology (NIST, 2020), when designing their security policies and processes, businesses should take into account the particular risks related to remote work.

In conclusion, remote working has emerged as a requirement for many businesses during the pandemic, but it also presents a unique set of security issues. Companies must establish efficient security solutions for remote workers, such as VPNs, security awareness training, MFA, and regular policy and procedure reviews, to safeguard critical data and stop cyberattacks. Companies may ensure that remote working is efficient and secure by adopting these actions.

Chapter 3: Methodology

3.1 Research Onion

3.1.2 Research Onion Overview

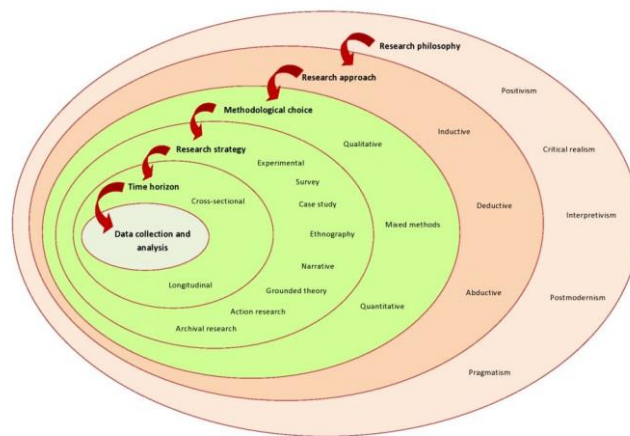


Figure 11 Research Onion

Saunders et al. (2012) developed the conceptual model known as The Research Onion for planning and carrying out research. It is referred to as a "onion" because it has layers that stack on top of one another to create a thorough research effort. The research onion is helpful because it enables researchers to arrange their research in a systematic manner and to organize their thoughts. The framework can be used with a variety of research approaches and offers a clear roadmap for the many stages of research, from the research philosophy to the gathering and analysis of data.

The research onion is a methodological framework that offers a systematic approach to detail the stages involved in the formulation of a research design. At its core, the onion metaphor signifies peeling away the layers to understand the various components of a research process, much like one would peel an onion. The outermost layer is the "Research Philosophy," which encompasses the beliefs and viewpoints about the nature and development of knowledge, often divided into epistemology and ontology. Once the researcher has a grasp of their philosophical stance, they move to the "Research Approach"

layer, which determines the logic behind the research. This could be deductive, starting with a theory and testing it, or inductive, starting with data and building a theory. Next is the "Research Choice" which pertains to the use of qualitative, quantitative, or mixed methods in the research. Following this is the "Research Strategy," where the researcher decides on the specific methodology, be it a survey, case study, experiment, etc., to best answer the research question. The "Time Horizon" layer follows, which pertains to whether the research is cross-sectional, taking place at a particular point in time, or longitudinal, occurring over an extended period. The innermost layer of the research onion is "Techniques and Procedures," which detail the specific methods and tools utilized for data collection and analysis. Navigating through each layer of the research onion ensures a holistic and thorough approach to designing research, ensuring all key components are considered and addressed.

3.1.2 Research Onion Layers

Research Philosophy layer encapsulates the foundational beliefs and viewpoints that guide the researcher in their understanding and interpretation of the world. Within this realm, several philosophies exist such as positivism (where the emphasis is on quantifiable observations leading to statistical analyses), interpretivism (focused on understanding the world from the individual's perspective), and realism (which acknowledges the existence of an external reality independent of human thoughts and beliefs). A researcher's choice of philosophy impacts their approach, methodology, and tools utilized in the research.

The Research Approach determines the progression of the research, specifically how a theory is developed or tested. Two primary approaches exist: deductive and inductive. A deductive approach begins with a theory or hypothesis and involves testing it, while the inductive approach starts with collecting data and subsequently formulates a theory based on the observed data. The chosen approach plays a significant role in directing the study's flow and determining its objectives.

At Research Choice layer, researchers decide whether they want to adopt a qualitative, quantitative, or mixed-method approach. Qualitative research delves deep into

understanding phenomena by exploring individual experiences, perceptions, or motivations. Quantitative research, on the other hand, aims to quantify the data and, typically, applies statistical analysis. Mixed-method involves a combination of both, allowing for a comprehensive exploration and quantification of research phenomena.

At Research Strategy layer, the researcher selects a specific methodology or design that aligns with the objectives of the research. Choices may include case studies (in-depth investigations of specific contexts or entities), surveys (gathering data from a large population using questionnaires or interviews), experiments (controlled investigations to understand cause-effect relationships), ethnography (studying cultural groups in their natural settings), and more. The strategy chosen paves the way for subsequent data collection and analysis procedures.

Time horizon layer pertains to the temporal aspect of the research. It can be cross-sectional, where data is gathered at a particular point in time, giving a snapshot of the phenomenon. Alternatively, it can be longitudinal, where data is collected over an extended period, allowing researchers to observe changes and developments over time. The selection between the two is influenced by the nature of the research question and the phenomena under study.

The Techniques and Procedures is the innermost layer of the research onion delves into the specifics of how data will be collected, analyzed, and interpreted. It encompasses the selection of sampling methods, data collection tools like interviews, questionnaires, or observations, and data analysis methods, which could range from statistical analyses to thematic analyses. The techniques and procedures ensure that the research is conducted systematically, yielding valid and reliable results.

Each layer of the research onion plays a pivotal role in shaping the research design, ensuring that the study is grounded in a robust methodological foundation, enabling the researcher to effectively address the research objectives.

3.2 Research Philosophy - Positivism

3.2.1 The chosen Research Philosophy

The Positivism philosophy was chosen for this study because it emphasizes the use of observable facts and scientific methods to investigate the security risks brought on by remote working at Lions Restoration Company. The research attempts to determine how Independent Variables (such as Company-sensitive data exposure, Employee-sensitive data exposure, Systems crashing issues, and Malicious issues) impact the company's security while employees operate remotely.

The research will investigate whether exposing company-sensitive data affects security risks during remote work. Also, determine whether exposing employee-sensitive data affects security risks while remote work. Then, examine whether system crashes affect security issues while remote work. Then, investigate into whether malicious activities (such as hacking) have an impact on remote work security. Likewise, the research aims to find a single, objective truth regarding the causes of security risks in remote working at the organization by examining these relationships between independent variables and dependent variable.

The study aims to find the connections between these variables and Lions Restoration Company's security concerns by collecting data and using analytical techniques. By following the Positivism approach, the study aims to produce reliable and comprehensive results that can enhance the understanding of the security concerns connected to remote work at the company.

3.2.2 The reason for choosing Positivism of Research Philosophy

I chose Positivism for my research because it's like being a detective using clear clues and science to find answers. For my study about the security risks when people work from home at Lions Restoration Company, I needed to look at clear facts and data. With Positivism, I can focus on things that I can see, measure, and test, like how often certain security

problems happen and why. I wanted to understand if issues like Company-sensitive data exposure, Employee-sensitive data exposure, Systems crashing issues, and Malicious issues affect the safety of work done remotely. By using Positivism, I can gather solid data and then analyze it to see if there's a link between these issues and the overall safety when employees work from home.

Now, there are other methods I could have chosen, but they didn't fit well for this study. Interpretivism wasn't picked because it's more about understanding people's feelings and opinions. It's like trying to find out how someone feels about their favorite food, instead of just finding out what their favorite food is. Since I was focused on clear data, not feelings or opinions, this method wasn't the best choice.

Realism mixes both feelings and clear data. But, it can be confusing for this kind of study because it tries to look at both what is real and how people feel about it. For my study, I just wanted the real facts, not feelings.

So, to keep things clear and straightforward, Positivism was the best choice. It lets me use real data to find out how safe it is for employees at Lions Restoration Company to work from home.

3.3 Research Approach - Deductive

3.3.1 The chosen Research Approach

There are two types of research approaches: inductive and deductive. The inductive approach focuses on developing new ideas by identifying patterns in data, whereas the deductive approach examines the validity of existing theories in specific circumstances or settings.

For this research, the independent variables (Company-sensitive data exposure, Employee-sensitive data exposure, Systems crashing issues, and Malicious issues) will be tested to determine if they affect the dependent variable (Security issues of remote working at Lions Restoration Company) within the company's environment and conditions. These independent variables have already been proven to influence security issues in remote

working in other countries, companies, or industries. The purpose of this study is to see if these variables have a comparable effect on remote working security issues, specifically in the unique environment of Lions Restoration Company.

The study will use a deductive approach to achieve this purpose. This means that the research will test the existing theories and hypotheses related to the independent variables and their impact on remote working security issues within the unique environment and conditions of Lions Restoration Company.

For numerous reasons, the deductive approach is preferred over the inductive approach. First off, theories and frameworks in use already point to a connection between the independent and dependent variables. Using the the deductive approach enables for evaluating these theories in the unique context of Lions Restoration Company to see if they hold true in this case. Second, the deductive approach gives a clear and focused study aim because it involves evaluating particular hypotheses derived from existing theories. This enables a more focused analysis of the correlations between the variables in the context of Lions Restoration Company, giving more accurate and relevant results. Finally, when compared to developing new theories using the inductive approach, testing existing theories using the deductive approach can save both time and money. Because the independent and dependent variables are already well-established in other contexts, it seems sensible to evaluate these correlations inside the Lions Restoration Company environment before attempting to create new theories.

By selecting the deductive approach, the research will efficiently and effectively test the existing theories related to the independent variables and their impact on the security issues of remote working within the specific environment and conditions of Lions Restoration Company. This approach will provide significant insights and contribute to the better understanding of security issues in remote working within the company's unique context.

3.3.2 The reason for choosing Deductive of Research Approach

I decided to go with the Deductive approach for my research because it's like using a trusted recipe to bake a cake but tweaking it a bit to suit a specific taste. When we talk about

research, there are two main approaches. One is Inductive, where we start with observations and then develop theories based on those observations. It's like noticing a lot of people enjoy sweet things, and then coming up with a theory that people generally like desserts.

On the other hand, Deductive is about starting with an existing theory and then testing it in a specific situation. In the context of my study, I'm using already known ideas (like how certain problems might impact the safety of working from home) and testing them specifically at Lions Restoration Company. We know from other places that issues like Company-sensitive data exposure, Employee-sensitive data exposure, Systems crashing issues, and Malicious issues can affect remote work safety. I want to see if these same issues are relevant and how they play out at Lions Restoration Company.

Now, I could have gone the Inductive way, which is like creating a new recipe from scratch after tasting a lot of dishes. But for my study, I already had some theories and ideas I wanted to test. This is why the Deductive approach, which is more like tweaking a tried-and-tested recipe, was better.

Using the Deductive approach means I'm testing known ideas in a new setting, which can give clearer and quicker insights. It's more focused since I'm not starting from scratch, and it can save both time and effort. Additionally, since these ideas have already been tested elsewhere, there's a higher chance of getting reliable results even in the unique setting of Lions Restoration Company.

While the Inductive approach has its merits, especially if we're exploring something entirely new or unique, it wasn't the best fit for this research. My goal was to see how known problems affect the specific environment of Lions Restoration Company. So, going Deductive made the most sense and was the most efficient way to get the answers I needed.

3.4 Research Choice – Mono Method Quantitative

3.4.1 The chosen Research Choice

The research choice for this study is a mono-method quantitative, which aligns with the selected Positivism philosophy and the deductive approach. A questionnaire allows for the collect of quantitative data and objective measurements, both of which are required for verifying current theories within the environment of Lions Restoration Company. This questionnaire allows respondents to answer as options that range from 1 (Strongly Disagree) to 5 (Strongly Agree) as per the Likert Scaler.

By adopting a mono-method quantitative research choice, the study will maintain consistency and standardization in data collection, helping to ensure reliable and valid results. This research choice contributes significantly to a consistent and well-structured research of the connections between the independent variables and the dependent variable, ultimately enhancing the understanding of security issues in remote working within the company's unique context.

3.4.2 The reason for choosing Mono Method Quantitative of Research Choice

Choosing the Mono Method Quantitative research choice for my study was like choosing to measure the ingredients for a cake using a single, precise method. Here's my explanation for this choice.

In research, how we gather and analyze data can take various paths. For my study, I wanted a clear, straightforward, and unbiased view of how certain problems might impact remote working at Lions Restoration Company. Hence, I went with the Mono Method Quantitative approach.

This approach means I am relying solely on numbers and structured data to get my answers. Think of it like a survey where you're asked to rate something on a scale of 1 to 5. I'm using a questionnaire that taps into this very idea. Respondents rate their agreement with various statements, using a scale where 1 means "Strongly Disagree" and 5 means "Strongly

Agree." This method ensures that every response can be easily translated into measurable data.

Why not other methods? Well, qualitative methods, like interviews or focus groups, although insightful, can sometimes introduce personal biases and are harder to standardize. I wanted something more straightforward and unbiased. Other mixed methods, which combine both qualitative and quantitative data, while comprehensive, can be time-consuming and might add complexity to the research process. Given my objectives and the need for consistency, these methods didn't seem the right fit.

Using the Mono Method Quantitative approach ensures that the data collected is consistent across all participants. This standardization is crucial, especially when trying to make sense of how known issues play out in a specific environment like Lions Restoration Company.

In summary, by opting for a purely quantitative approach, I aimed for a research path that was clear, concise, and unbiased. This way, I can get straightforward insights into the relationship between the selected issues and remote working security at the Lions Restoration Company.

3.5 Research Strategy – Mono Method Questionnaire

3.5.1 The chosen Research Strategy

To collect quantitative data in this study, a mono-method questionnaire research strategy is used since we are using mono-method quantitative research choice. A survey is being used to collect data from the sample. Due to factors like the cost, time, respondent availability, and complexity, a survey method is used instead of a census. A census would require collecting data from every member of the population, which can be time-consuming, expensive, and logistically challenging. A survey, on the other hand, allows for a smaller sample size while still giving useful information.

A questionnaire is used for gathering responses from the participants, providing an organized and effective method for collecting data. The Likert scale is used for respondents to rate their views, with options that range from 1 (Strongly Disagree) to 5 (Strongly

Agree). This method allows the researcher to collect participants' opinions and views in a standardized and easily analyzed manner, helping the analysis of relationships between the variables in the study.

3.5.2 The reason for choosing Mono Method Questionnaire of Research Strategy

Choosing the Mono Method Questionnaire for my Research Strategy was a calculated decision, analogous to an architect choosing bricks for the foundation, knowing they offer both stability and uniformity. Research, in many ways, is about asking questions and finding answers. But how we pose these questions and in which context can significantly change the results we get. In my quest to understand security issues related to remote working at Lions Restoration Company, I found the Mono Method Questionnaire to be the best fit.

Why this strategy? First and foremost, questionnaires are precise. Each participant receives the same set of questions, framed in the same way. This uniformity ensures that each response is based on the same understanding, limiting any interpretative biases. Additionally, using the Likert scale (where 1 means "Strongly Disagree" and 5 means "Strongly Agree") offers a straightforward way for participants to express their opinions, ensuring that the data can be easily quantified and analyzed.

But why not other methods? Experimentations or case studies, for example, are comprehensive, but they might not be feasible given the constraints I had regarding time, budget, and the nature of the study. Observations or longitudinal studies would require a more extended interaction with the participants, which might not always be possible, especially in a corporate setting. Plus, getting in-depth qualitative insights, while valuable, might not align with the primarily quantitative nature of this study.

Another key aspect was the choice of a survey over a census. Imagine trying to get feedback from every single employee of a large company. It's not only time-consuming and costly but might also be redundant. With a well-constructed survey, I could glean insights from a representative sample, thus making the data collection process efficient and still providing reliable results.

In conclusion, the Mono Method Questionnaire strategy was chosen for its clarity, efficiency, and precision. By focusing on a survey-based questionnaire, I hoped to get a clear snapshot of the perceptions and experiences of the employees of Lions Restoration Company concerning the security challenges of remote working. This approach, I believe, paves the way for robust, insightful, and actionable findings.

3.6 Time Horizon – Cross Sectional

3.6.1 The chosen Time Horizon

In this study, the research involves collecting quantitative data through a quantitative questionnaire. The full study, including data collecting and analysis, is projected to be completed in less than 10 months. Each participant will only be needed to provide data once, and the data collection process per individual is estimated to take less than 30 minutes. Based on these factors, the research employs a cross-sectional time horizon, which enables efficient data analysis at a single point in time.

3.6.2 The reason for choosing Cross Sectional of Time Horizon

The decision to opt for a Cross-Sectional time horizon in this research was influenced by the nature and scope of the study, aiming to capture the current dynamics of security issues in remote working at Lions Restoration Company. The cross-sectional design, which studies a specific subject at a single point in time, seemed most apt considering the study's parameters and requirements.

To understand this choice, it's crucial to be familiar with the alternatives and their implications. Longitudinal studies, another popular time horizon, involve multiple observations over extended periods. Such designs are typically chosen for studying trends, developments, or evolutions. However, in the context of this study, that approach would have been like using a telescope when binoculars would do. The longitudinal design might have shed light on how security issues evolve or change over time, but it would have also

meant more extended interaction with participants, increasing costs, and logistical challenges, especially since the study's main objective was to capture a snapshot of the current situation.

Considering the specific parameters I outlined for this research, such as the quantitative data collection through questionnaires and the projection of completion in under 10 months, a cross-sectional time horizon was the logical choice. It promises efficiency, ensuring participants are not overburdened (given they'd spend less than 30 minutes) and the study remains within its set timeline.

Moreover, this approach was also influenced by the ever-evolving nature of remote work practices and security challenges. In such a dynamic field, a snapshot provides a valuable insight into current practices and challenges, which can be crucial for Lions Restoration Company to address its immediate needs. A longitudinal study, while rich in data, might have delayed actionable insights.

In summary, the choice of a cross-sectional time horizon was driven by the desire for efficiency, the nature of the research question, the dynamic environment of remote working, and the constraints of time and resources. This approach allows the study to present a concise, clear, and timely depiction of security issues in remote working at Lions Restoration Company at this specific juncture.

3.7 Techniques and Procedures

3.7.1 Target Population

The target population for this research consists of all remote working employees at Lions Restoration Company in Sri Lanka. There are 60 employees in total. To conduct the research, all 60 remote working employees from the company in Sri Lanka will be selected as the Target Population, ensuring that the study captures the perspectives and experiences of the entire remote workforce within the organization's Sri Lankan branch.

3.7.2 Sample Population

In some research contexts, it can be challenging to collect data from the entire target population due to cost, approaching issues, and time constraints. As a result, a sample is often selected from the target population to conduct the study. However, in this research, the total population of remote working employees at Lions Restoration Company in Sri Lanka is 60, and according to Morgan's Table, the minimum sample size is 52. This means at least 52 respondents should be included in the study to gather information on the research topic. Given these factors, it is feasible to include at least 52 employees from the target population in the sample size. Therefore, 55 remote-working employees of Lions Restoration Company in Sri Lanka will be selected as the sample for this study. The developed questionnaire will be delivered to the sample population, and the research results will be dependent on the responses obtained from these respondents.

3.7.3 Data collection Method

There are two methods that can be used to deliver a questionnaire: an online-based method and a paper-based method. In this research, the online-based method using Google Forms is selected due to its cost-effectiveness and convenience. The questionnaire is designed to represent the independent and dependent variables, utilizing a Likert scale for the response options. This scale assigns ratings from 1 to 5, with 1 indicating "Strongly Disagree," 2 representing "Disagree," 3 being "Neutral," 4 signifying "Agree," and 5 denoting "Strongly Agree."

By using an online-based questionnaire with Likert scale questions, the research can effectively gather data on the relationships between the independent and dependent variables in a user-friendly and efficient manner.

3.7.4 The reason for choosing online-based method as Data collection Method

The online-based method for data collection, specifically through Google Forms, was my top choice for several compelling reasons. Given the research's topic of remote working and its associated security challenges, it felt instinctively right to mirror the same digital landscape in the data collection method. Furthermore, in light of the ongoing shift towards digitalization, online-based methods have become more acceptable and accessible to many respondents.

Contrastingly, traditional paper-based methods, while still effective in some contexts, present a set of challenges. Firstly, there's the obvious environmental concern of paper consumption. Moreover, in terms of logistics, distributing and collecting paper questionnaires can be cumbersome, especially if the participants are geographically spread out. This would also entail additional costs, both in terms of money (for printing and postage) and time (for distribution, collection, and then manual data input).

An online questionnaire, on the other hand, provides instant accessibility to participants wherever they may be. This instantaneity ensures timely responses, which, in turn, facilitates a smoother progression to the data analysis phase. It also allows for real-time monitoring of response rates, easy follow-ups, and the capability to make minor adjustments if necessary.

Additionally, the current research, which revolves around the challenges faced by a company employing remote working, naturally suggests that its employees are already accustomed to digital tools. Thus, an online method aligns with their usual way of functioning, making it convenient for them to respond. Furthermore, data collected online can be directly fed into analytical software, reducing the risk of manual data entry errors.

Another notable advantage of online methods is the ease of scalability. While a paper-based survey is restricted by physical resources, an online survey can be sent to hundreds or even thousands of respondents at virtually no additional cost.

While there might be some concerns about digital literacy or access to reliable internet connections, considering the research's focus on a digitally forward company like Lions Restoration, these concerns are likely minimal.

In essence, the decision to adopt an online-based method for data collection was rooted in practicality, efficiency, and relevance to the study's topic. The digital method, especially using a widely recognized platform like Google Forms, ensures broad accessibility, quick responses, and efficient data handling, which are all pivotal in guaranteeing the research's success.

3.7.5 Data Analysis

Upon receiving the completed questionnaires, the results will be entered into Microsoft Excel for data analysis. The software will be used to perform various statistical techniques, including Regression Analysis, Descriptive Statistics, and Correlation Analysis, to generate insightful results. Additionally, graphical representation methods such as pie charts and bar charts will be employed to visualize the data and further enhance the understanding of the relationships between the independent and dependent variables. This comprehensive approach to data analysis will provide a solid foundation for interpreting the research findings and drawing meaningful conclusions.

3.8 Research Limitation

This research has several limitations that may affect its findings. Secondly, time constraints limit the study's depth and scope, potentially influencing the quality of data collecting and analysis. Second, a limited budget limits the resources available for conducting research, which may have an impact on the quality of the techniques and methods used. Access to supervisors and officers within the company is challenging, potentially limiting the diversity of perspectives and insights gathered. Language barriers may also be an issue, causing misunderstandings or misinterpretations of the questions or responses. Additionally, the respondents' various psychological states may alter their thoughts and opinions, which the questionnaire may not fully capture. Other limitations may include the small sample size, which is restricted to at least 52 remote employees at Lions Restoration Company in Sri Lanka. This could limit the generalizability of the findings to a broader

context or other organizations. Additionally, the use of a mono-method questionnaire may not capture the full complexity of the relationships between the variables, as it primarily focuses on quantitative data.

Furthermore, participants who provide socially desired answers or who are affected by personal ideas or opinions may have an impact on the results acquired. Nonresponse bias may also occur if some participants choose not to respond to the questionnaire or drop out of the study, potentially skewing the results and restricting the findings' generalizability. The research's quantitative approach may not reflect the full complexity and richness of remote working and security challenges. The research results might be better accurate if qualitative data were included. Furthermore, there may be unexpected external forces or variables unaccounted for in the research that could unexpectedly influence the relationships between the independent and dependent variables. Finally, the implementation of an online-based questionnaire may result in technical difficulties or limited internet connection, potentially influencing the response rate and the quality of the data obtained.

Despite these limitations, the research aims to provide valuable insights into the security issues related to remote working at Lions Restoration Company and contribute to the understanding of the factors influencing these issues within the company's specific context.

3.9 Research Ethics

In this research, abiding to ethical guidelines is vital to safeguard the participants and maintain the integrity of the study. Firstly, acquiring informed consent from the participants ensures that they voluntarily agree to participate and fully comprehend the research's purpose and nature. The study will exclude persons over the age of 60 and minors under the age of 18 because their psychological situations may make it difficult for them to provide accurate data. Additionally, no personal data will be collected, preserving the participants' privacy and confidentiality. The findings of the study will not be used for commercial purposes, emphasizing that they are only for academic and organizational improvement. Further ethical considerations include being transparent about the research

objectives, preserving honesty in data collecting and analysis, and addressing any potential biases or limitations in the study.

This study should prioritize the well-being of the participants, ensuring that they suffer no physical or psychological injury. The research must be conducted with the utmost care to reduce any potential discomfort or suffering. Furthermore, secure data storage and management are critical to preventing unauthorized access or misuse. Adhering to relevant data protection regulations and ensuring the proper disposal of data after the study's completion are essential steps in maintaining the integrity of the research. Furthermore, the research should be respectful to the participants' cultural origins and perspectives. When designing the questionnaire and interpreting the data, I should make an attempt to understand and respect cultural variations. Finally, all applicable laws, regulations, and institutional requirements must be followed, including getting ethical review board clearance and adhering to data protection rules.

By adhering to these ethical guidelines, the research aims to provide a trustworthy and reliable investigation into the security issues related to remote working at Lions Restoration Company, while respecting the rights and well-being of the participants involved.

3.10 Accuracy and Validity of the Research

Many measures are used to ensure the research's accuracy and validity. To begin, there is no manipulation from the research to the participants, ensuring that the data collected accurately represents the respondents' viewpoints and experiences. Second, a pilot study was carried out to validate the questionnaire, helping to optimize the survey instrument and ensure that the questions are clear, relevant, and appropriately designed to capture the necessary information.

Furthermore, the research follows ethical guidelines, such as maintaining neutrality and impartiality during data collecting and analysis, which improves the accuracy and validity of the results. Moreover, the use of reliable statistical techniques, such as regression analysis, descriptive statistics, and correlation analysis, contributes to the credibility of the

findings. The study also identifies and addresses potential limits, encouraging a more honest and realistic perspective on the scope and reliability of the research.

By using these steps, the research hopes to ensure that its findings are reliable, valid, and provide to a better understanding of the security risks associated with remote working at Lions Restoration Company.

Chapter 4: Analysis

4.1 Presentation of Data

4.1.1 Presentation of Data for Entire Company-Sensitive Data Exposure

4.1.1.1 Presentation of Data for Entire Question 1- Do you have access to company-sensitive data in your remote work?

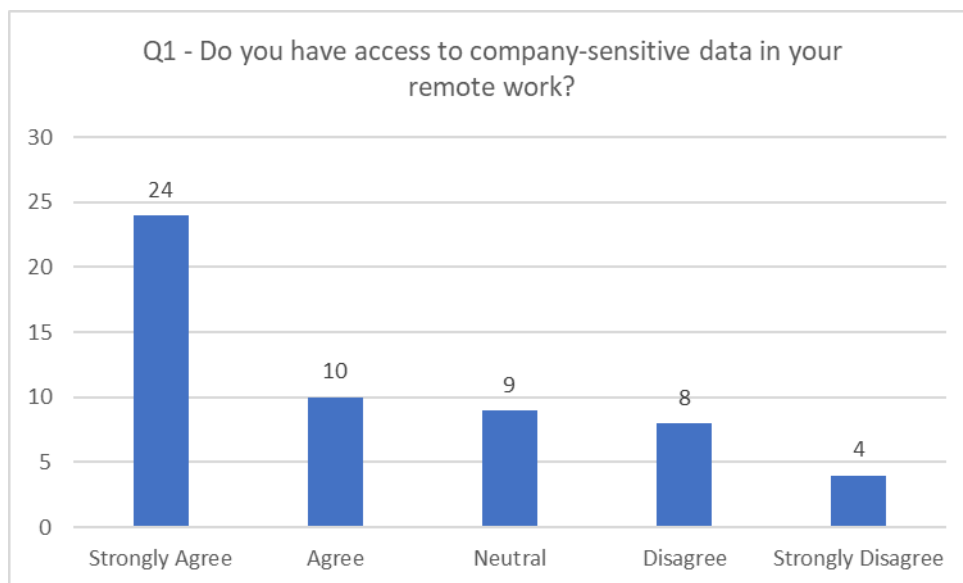


Figure 12 Presentation of Data for Entire Question 1- Do you have access to company-sensitive data in your remote work?

For the Question “Do you have access to company-sensitive data in your remote work?”, the maximum number of responses is 24 for Strongly Agree and the minimum number of responses is 4 for Strongly Disagree. And the majority of responses appear to be on the Agree side.

4.1.1.2 Presentation of Data for Entire Question 2- Aren't you confident about the security measures in place to protect company-sensitive data while working remotely?

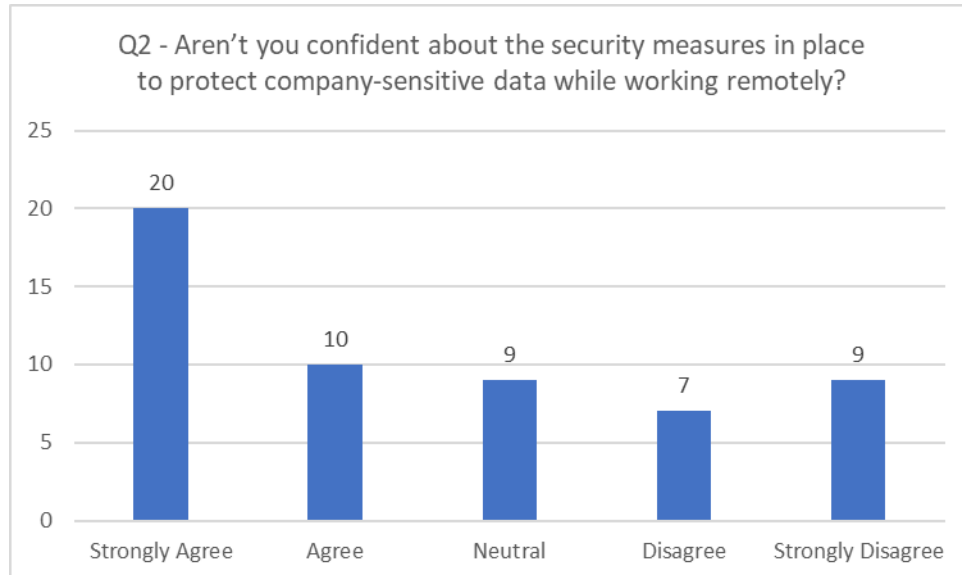


Figure 13 Presentation of Data for Entire Question 2- Aren't you confident about the security measures in place to protect company-sensitive data while working remotely?

For the question "Aren't you confident about the security measures in place to protect company-sensitive data while working remotely?", the maximum number of responses is 20 for Strongly Agree and the minimum number of responses is 7 for Disagree. And the majority of responses appear to be on the Agree side.

4.1.1.3 Presentation of Data for Entire Question 1- Do you believe that company-sensitive data is likely to be exposed due to remote working?

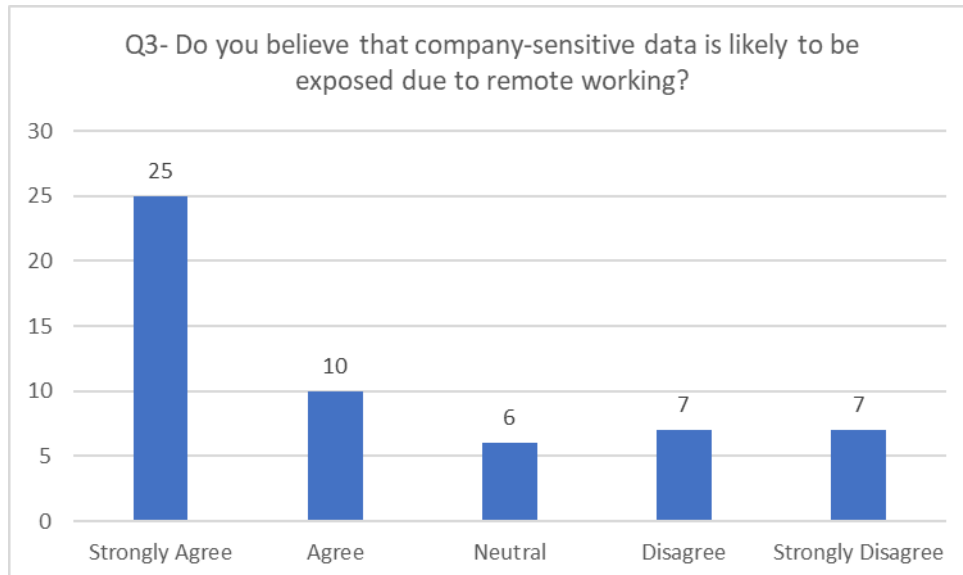


Figure 14 Presentation of Data for Entire Question 1- Do you believe that company-sensitive data is likely to be exposed due to remote working?

For the question "Do you believe that company-sensitive data is likely to be exposed due to remote working?", the maximum number of responses is 25 for Strongly Agree and the minimum number of responses is 6 for Neutral. And the majority of responses appear to be on the Agree side.

4.1.1.4 Presentation of Data for Entire Question 1- Do you feel you and your fellow employees are not well-trained to protect company-sensitive data in a remote work environment?



Figure 15 Presentation of Data for Entire Question 1- Do you feel you and your fellow employees are not well-trained to protect company-sensitive data in a remote work environment?

For the question “Do you feel you and your fellow employees are not well-trained to protect company-sensitive data in a remote work environment?”, the maximum number of responses is 27 for Strongly Agree and the minimum number of responses is 4 for Neutral. And the majority of responses appear to be on the Agree side.

4.1.2 Presentation of Data for Entire Employee-Sensitive Data Exposure

4.1.2.1 Presentation of Data for Entire Question 1- Do you frequently provide personal information for work-related tasks while working remotely?

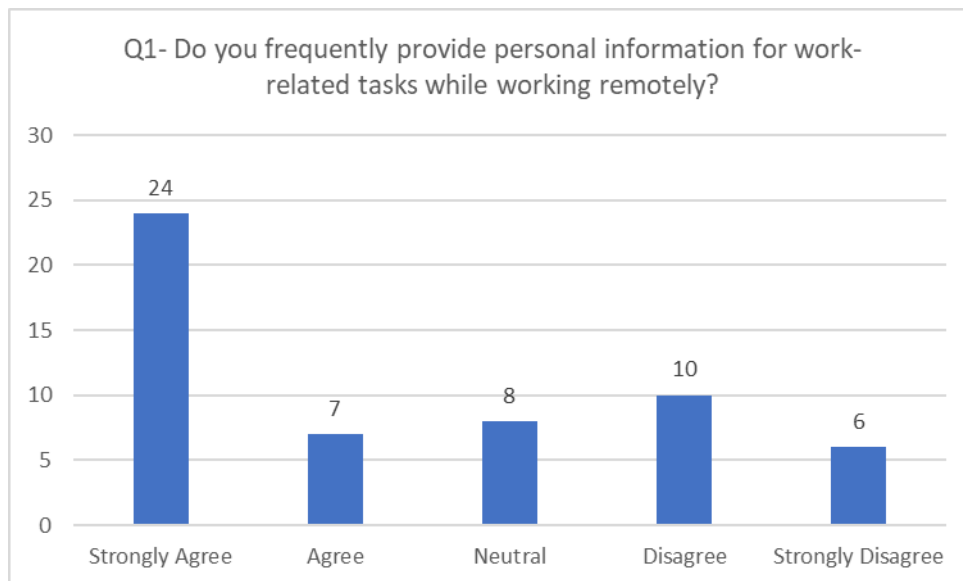


Figure 16 Presentation of Data for Entire Question 1- Do you frequently provide personal information for work-related tasks while working remotely?

For the question " Do you frequently provide personal information for work-related tasks while working remotely?", the maximum number of responses is 24 for Strongly Agree and the minimum number of responses is 6 for Strongly Disagree. And the majority of responses appear to be on the Agree side.

4.1.2.2 Presentation of Data for Entire Question 1- Aren't you confident about the security measures in place to protect your personal data while working remotely?



Figure 17 Presentation of Data for Entire Question 1- Aren't you confident about the security measures in place to protect your personal data while working remotely?

For the question " Aren't you confident about the security measures in place to protect your personal data while working remotely?", the maximum number of responses is 18 for Strongly Agree and the minimum number of responses is 7 for Neutral. And the majority of responses appear to be on the Agree side.

4.1.2.3 Presentation of Data for Entire Question 1- Do you believe that your personal data is likely to be exposed due to remote working?

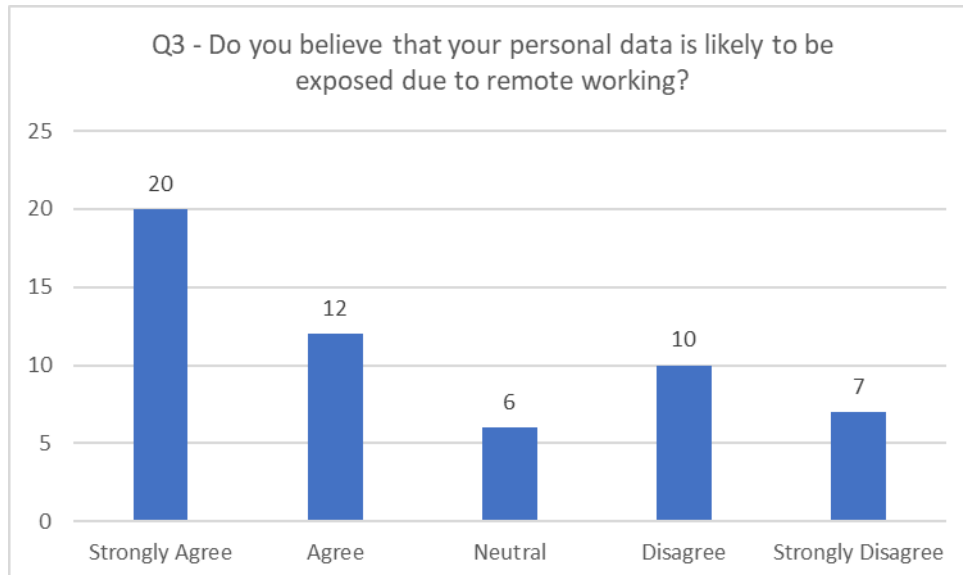


Figure 18 Presentation of Data for Entire Question 1- Do you believe that your personal data is likely to be exposed due to remote working?

For the question "Do you believe that your personal data is likely to be exposed due to remote working?", the maximum number of responses is 20 for Strongly Agree and the minimum number of responses is 6 for Neutral. And the majority of responses appear to be on the Agree side.

4.1.2.4 Presentation of Data for Entire Question 1- Do you feel you and your fellow employees are not well-educated about protecting personal data in a remote work environment?

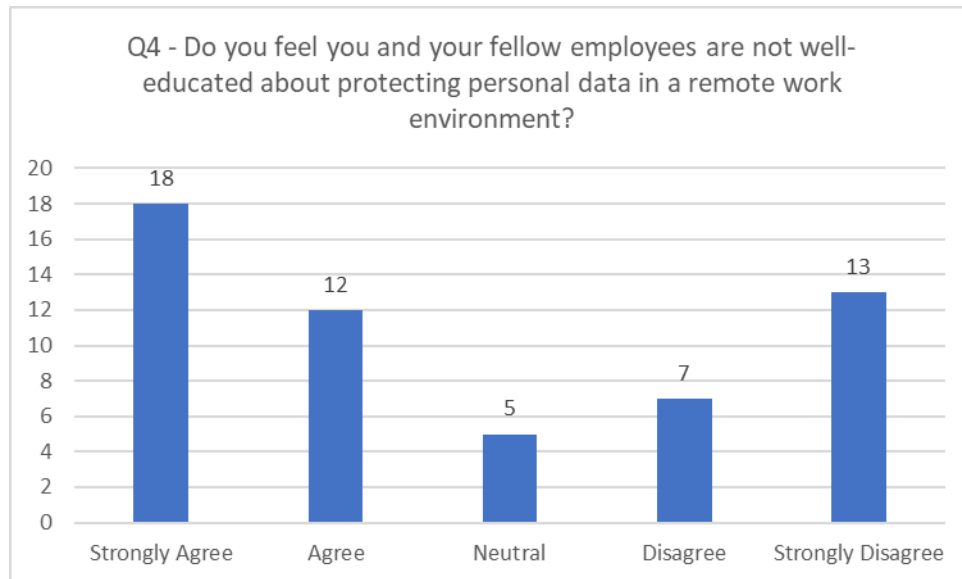


Figure 19 Presentation of Data for Entire Question 1- Do you feel you and your fellow employees are not well-educated about protecting personal data in a remote work environment?

For the question "Do you feel you and your fellow employees are not well-educated about protecting personal data in a remote work environment?", the maximum number of responses is 18 for Strongly Agree and the minimum number of responses is 5 for Neutral. And the majority of responses appear to be on the Agree side.

4.1.3 Presentation of Data for Entire Systems Crashing Issues

4.1.3.1 Presentation of Data for Entire Question 1- How frequently have you experienced system crashes while working remotely?

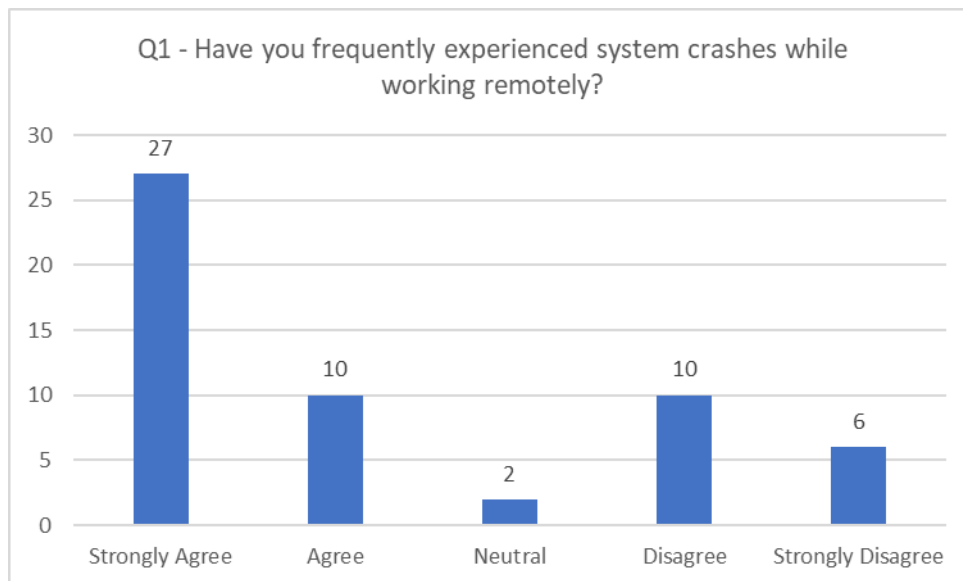


Figure 20 Presentation of Data for Entire Question 1- How frequently have you experienced system crashes while working remotely?

For the question "How frequently have you experienced system crashes while working remotely?", the maximum number of responses is 27 for Strongly Agree and the minimum number of responses is 2 for Neutral. And the majority of responses appear to be on the Agree side.

4.1.3.2 Presentation of Data for Entire Question 1- Aren't you confident in the company's ability to quickly address system crashes that occur during remote work?

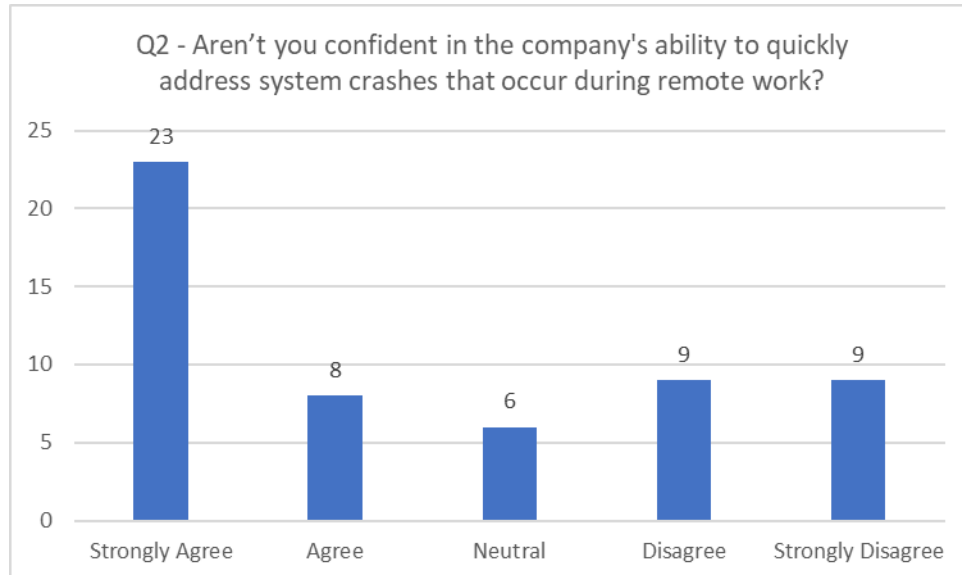


Figure 21 Presentation of Data for Entire Question 1- Aren't you confident in the company's ability to quickly address system crashes that occur during remote work?

For the question "Aren't you confident in the company's ability to quickly address system crashes that occur during remote work?", the maximum number of responses is 23 for Strongly Agree and the minimum number of responses is 6 for Neutral. And the majority of responses appear to be on the Agree side.

4.1.3.3 Presentation of Data for Entire Question 1- Do you believe system crashes could likely lead to security issues in a remote work environment?

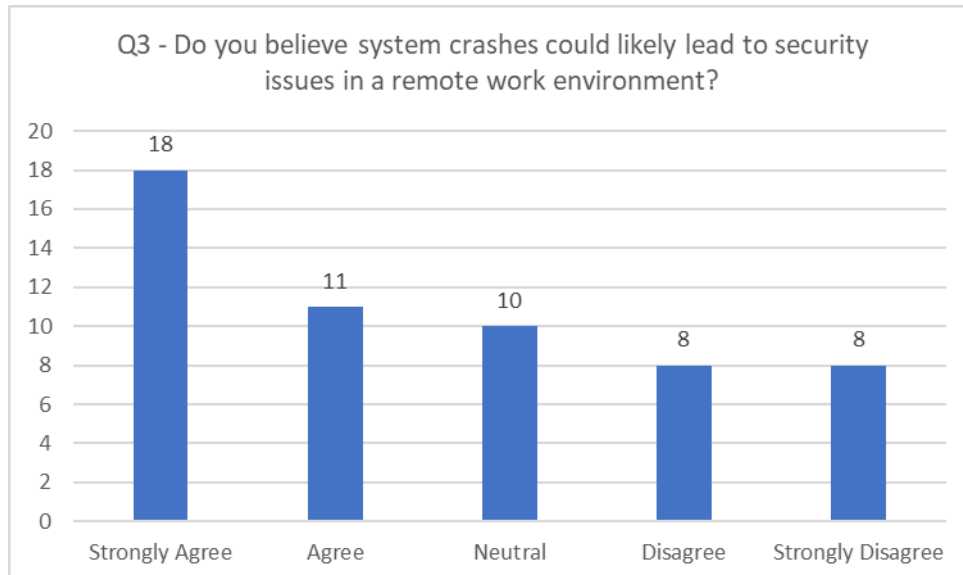


Figure 22 Presentation of Data for Entire Question 1- Do you believe system crashes could likely lead to security issues in a remote work environment?

For the question "Do you believe system crashes could likely lead to security issues in a remote work environment?", the maximum number of responses is 18 for Strongly Agree and the minimum number of responses is 8 for both Disagree and Strongly Disagree. And the majority of responses appear to be on the Agree side.

4.1.3.4 Presentation of Data for Entire Question 1- Do you feel you and your fellow employees are not well-prepared to respond to system crashes in a remote work environment?

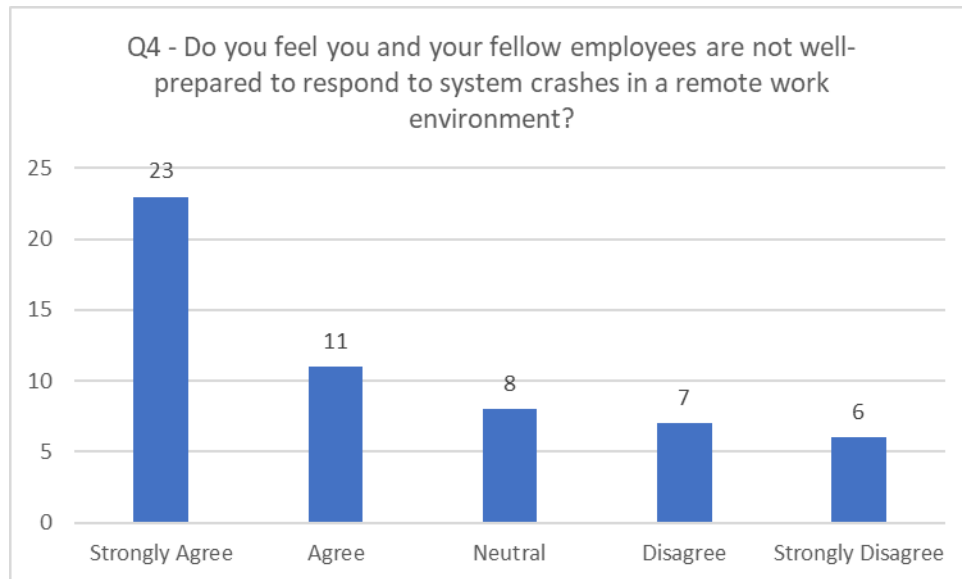


Figure 23 Presentation of Data for Entire Question 1- Do you feel you and your fellow employees are not well-prepared to respond to system crashes in a remote work environment?

For the question " Do you feel you and your fellow employees are not well-prepared to respond to system crashes in a remote work environment?", the maximum number of responses is 23 for Strongly Agree and the minimum number of responses is 6 for Strongly Disagree. And the majority of responses appear to be on the Agree side.

4.1.4 Presentation of Data for Entire Malicious Issues

4.1.4.1 Presentation of Data for Entire Question 1- Have you frequently encountered or heard about malicious activities (e.g., phishing, malware) while working remotely?

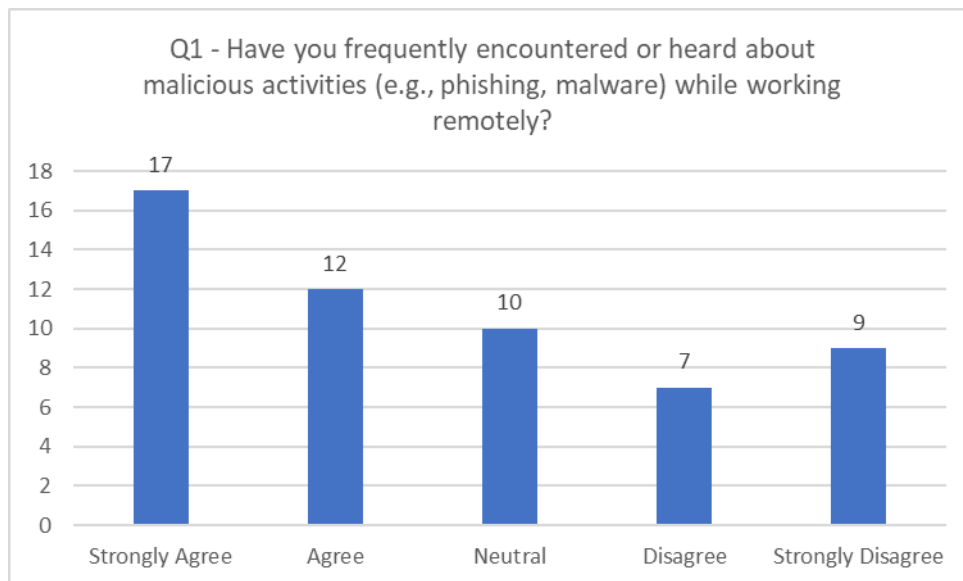


Figure 24 Presentation of Data for Entire Question 1- Have you frequently encountered or heard about malicious activities (e.g., phishing, malware) while working remotely?

For the question “Have you frequently encountered or heard about malicious activities (e.g., phishing, malware) while working remotely?”, the maximum number of responses is 17 for Strongly Agree and the minimum number of responses is 7 for Disagree. And the majority of responses appear to be on the Agree side.

4.1.4.2 Presentation of Data for Entire Question 1- Aren't you confident in the company's ability to prevent or address malicious activities during remote work?

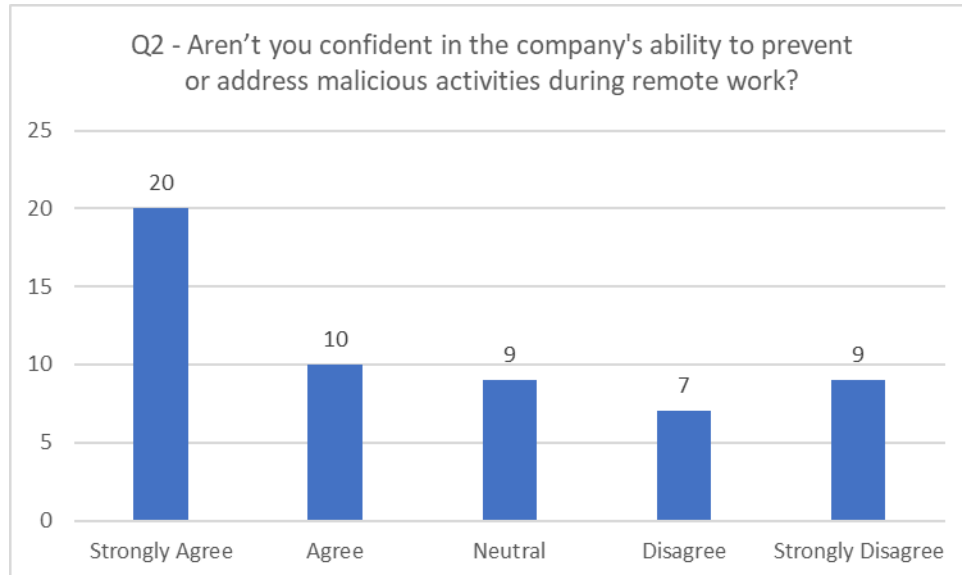


Figure 25 Presentation of Data for Entire Question 1- Aren't you confident in the company's ability to prevent or address malicious activities during remote work?

For the question "Aren't you confident in the company's ability to prevent or address malicious activities during remote work?", the maximum number of responses is 20 for Strongly Agree and the minimum number of responses is 7 for Disagree. And the majority of responses appear to be on the Agree side.

4.1.4.3 Presentation of Data for Entire Question 1- Do you believe malicious activities could likely lead to security issues in a remote work environment?

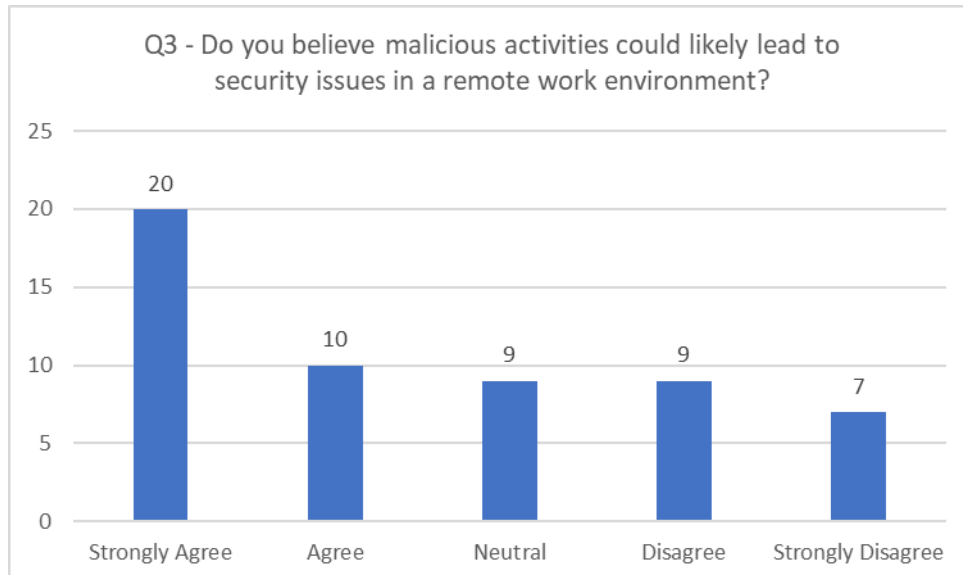


Figure 26 Presentation of Data for Entire Question 1- Do you believe malicious activities could likely lead to security issues in a remote work environment?

For the question "Do you believe malicious activities could likely lead to security issues in a remote work environment?", the maximum number of responses is 20 for Strongly Agree and the minimum number of responses is 7 for Strongly Disagree. And the majority of responses appear to be on the Agree side.

4.1.4.4 Presentation of Data for Entire Question 1- Do you feel you and your fellow employees are not well-trained to identify and avoid malicious activities in a remote work environment?

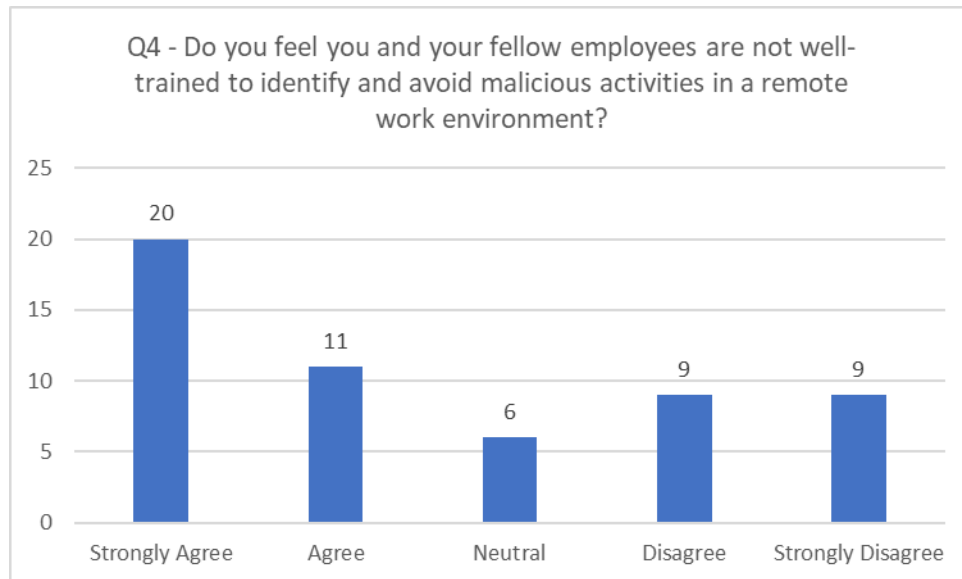


Figure 27 Presentation of Data for Entire Question 1- Do you feel you and your fellow employees are not well-trained to identify and avoid malicious activities in a remote work environment?

For the question "Do you feel you and your fellow employees are not well-trained to identify and avoid malicious activities in a remote work environment?", the maximum number of responses is 20 for Strongly Agree and the minimum number of responses is 6 for Neutral. And the majority of responses appear to be on the Agree side.

4.1.5 Presentation of Data for Entire Security Issues of Remote Working at Lions Restoration Company

4.1.5.1 Presentation of Data for Entire Question 1- Overall, how dissatisfied are you with the level of security issues associated with remote work at Lions Restoration Company

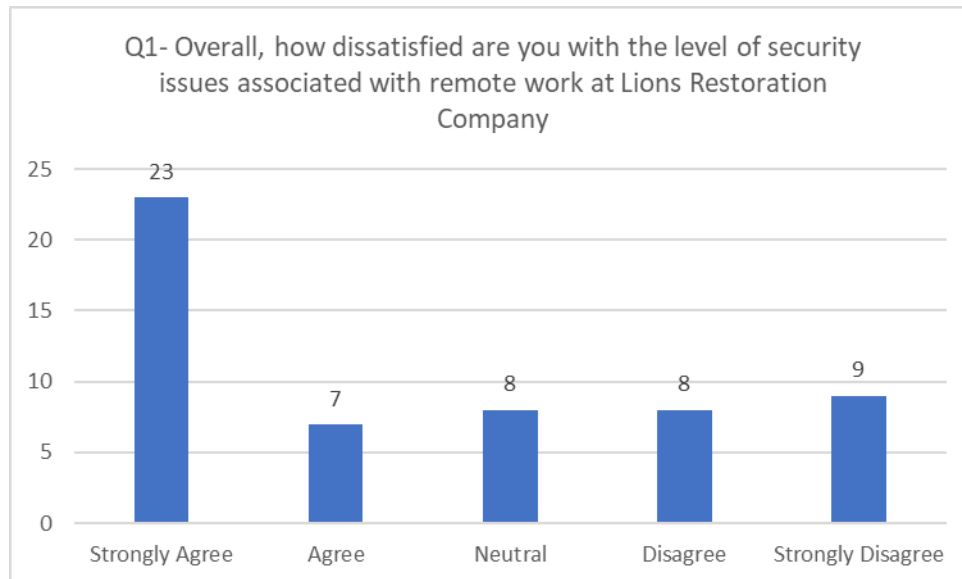


Figure 28 Presentation of Data for Entire Question 1- Overall, how dissatisfied are you with the level of security issues associated with remote work at Lions Restoration Company

For the question "Overall, how dissatisfied are you with the level of security issues associated with remote work at Lions Restoration Company ", the maximum number of responses is 23 for Strongly Agree and the minimum number of responses is 7 for Agree. And the majority of responses appear to be on the Agree side.

4.2 Descriptive Statistics

4.2.1 Descriptive Statistics for Entire Company-Sensitive Data Exposure

Table 1 Descriptive Statistics for Entire Company-Sensitive Data Exposure

	Min	Max	Mean	S.D.
Q1	1	5	3.76	1.35
Q2	1	5	3.45	1.50
Q3	1	5	3.71	1.47
Q4	1	5	3.75	1.47

For the question “Do you have access to company-sensitive data in your remote work?” minimum and maximum responses are Strongly Disagree and Strongly Agree. So, the range of the answers are Strongly Disagree to Strongly Agree. Mean value for the question is 3.76. And it’s close to 4. Hence the general answers of the respondents are into Agree. And the standard deviation is 1.35.

For the question “Aren’t you confident about the security measures in place to protect company-sensitive data while working remotely?” minimum and maximum responses are Strongly Disagree and Strongly Agree. So, the range of the answers are Strongly Disagree to Strongly Agree. Mean value for the question is 3.45. And it’s close to 3. Hence the general answers of the respondents are into Neutral. And the standard deviation is 1.50.

For the question “Do you believe that company-sensitive data is likely to be exposed due to remote working?” minimum and maximum responses are Strongly Disagree and Strongly Agree. So, the range of the answers are Strongly Disagree to Strongly Agree. Mean value for the question is 3.71. And it’s close to 4. Hence the general answers of the respondents are into Agree. And the standard deviation is 1.47.

For the question “Do you feel you and your fellow employees are not well-trained to protect company-sensitive data in a remote work environment?” minimum and maximum responses are Strongly Disagree and Strongly Agree. So, the range of the answers are Strongly Disagree to Strongly Agree. Mean value for the question is 3.75. And it’s close to 4. Hence the general answers of the respondents are into Agree. And the standard deviation is 1.47.

4.1.2 Descriptive Statistics for Entire Employee-Sensitive Data Exposure

Table 2 Descriptive Statistics for Entire Employee-Sensitive Data Exposure

	Min	Max	Mean	S.D.
Q1	1	5	3.60	1.47
Q2	1	5	3.20	1.60
Q3	1	5	3.51	1.46
Q4	1	5	3.27	1.60

For the question “Do you frequently provide personal information for work-related tasks while working remotely?” minimum and maximum responses are Strongly Disagree and Strongly Agree. So, the range of the answers are Strongly Disagree to Strongly Agree. Mean value for the question is 3.60. And it’s close to 4. Hence the general answers of the respondents are into Agree. And the standard deviation is 1.47.

For the question “Aren’t you confident about the security measures in place to protect your personal data while working remotely?” minimum and maximum responses are Strongly Disagree and Strongly Agree. So, the range of the answers are Strongly Disagree to Strongly Agree. Mean value for the question is 3.20. And it’s close to 3. Hence the general answers of the respondents are into Neutral. And the standard deviation is 1.60.

For the question “Do you believe that your personal data is likely to be exposed due to remote working?” minimum and maximum responses are Strongly Disagree and Strongly Agree. So, the range of the answers are Strongly Disagree to Strongly Agree. Mean value for the question is 3.51. And it’s close to 4. Hence the general answers of the respondents are into Agree. And the standard deviation is 1.46.

For the question “Do you feel you and your fellow employees are not well-educated about protecting personal data in a remote work environment?” minimum and maximum responses are Strongly Disagree and Strongly Agree. So, the range of the answers are Strongly Disagree to Strongly Agree. Mean value for the question is 3.27. And it’s close to 3. Hence the general answers of the respondents are into Neutral. And the standard deviation is 1.60.

4.2.3 Descriptive Statistics for Entire Systems Crashing Issues

Table 3 Descriptive Statistics for Entire Systems Crashing Issues

	Min	Max	Mean	S.D.
Q1	1	5	3.76	1.49
Q2	1	5	3.49	1.56
Q3	1	5	3.42	1.45
Q4	1	5	3.69	1.41

For the question “Have you frequently experienced system crashes while working remotely?” minimum and maximum responses are Strongly Disagree and Strongly Agree. So, the range of the answers are Strongly Disagree to Strongly Agree. Mean value for the question is 3.76. And it’s close to 4. Hence the general answers of the respondents are into Agree. And the standard deviation is 1.49.

For the question “Aren’t you confident in the company's ability to quickly address system crashes that occur during remote work?” minimum and maximum responses are Strongly Disagree and Strongly Agree. So, the range of the answers are Strongly Disagree to Strongly Agree. Mean value for the question is 3.49. And it’s close to 3. Hence the general answers of the respondents are into Neutral. And the standard deviation is 1.56.

For the question “Do you believe system crashes could likely lead to security issues in a remote work environment?” minimum and maximum responses are Strongly Disagree and Strongly Agree. So, the range of the answers are Strongly Disagree to Strongly Agree. Mean value for the question is 3.42. And it’s close to 3. Hence the general answers of the respondents are into Neutral. And the standard deviation is 1.45.

For the question “Do you feel you and your fellow employees are not well-prepared to respond to system crashes in a remote work environment?” minimum and maximum responses are Strongly Disagree and Strongly Agree. So, the range of the answers are Strongly Disagree to Strongly Agree. Mean value for the question is 3.69. And it’s close to 4. Hence the general answers of the respondents are into Agree. And the standard deviation is 1.41.

4.2.4 Descriptive Statistics for Entire Malicious Issues

Table 4 Descriptive Statistics for Entire Malicious Issues

	Min	Max	Mean	S.D.
Q1	1	5	3.38	1.46
Q2	1	5	3.45	1.50
Q3	1	5	3.49	1.45
Q4	1	5	3.44	1.52

For the question “Have you frequently encountered or heard about malicious activities (e.g., phishing, malware) while working remotely?” minimum and maximum responses are Strongly Disagree and Strongly Agree. So, the range of the answers are Strongly Disagree to Strongly Agree. Mean value for the question is 3.38. And it’s close to 3. Hence the general answers of the respondents are into Neutral. And the standard deviation is 1.46.

For the question “Aren’t you confident in the company's ability to prevent or address malicious activities during remote work?” minimum and maximum responses are Strongly Disagree and Strongly Agree. So, the range of the answers are Strongly Disagree to Strongly Agree. Mean value for the question is 3.45. And it’s close to 3. Hence the general answers of the respondents are into Neutral. And the standard deviation is 1.50.

For the question “Do you believe malicious activities could likely lead to security issues in a remote work environment?” minimum and maximum responses are Strongly Disagree and Strongly Agree. So, the range of the answers are Strongly Disagree to Strongly Agree. Mean value for the question is 3.49. And it’s close to 3. Hence the general answers of the respondents are into Neutral. And the standard deviation is 1.45.

For the question “Do you feel you and your fellow employees are not well-trained to identify and avoid malicious activities in a remote work environment?” minimum and maximum responses are Strongly Disagree and Strongly Agree. So, the range of the answers are Strongly Disagree to Strongly Agree. Mean value for the question is 3.44. And it’s close to 3. Hence the general answers of the respondents are into Neutral. And the standard deviation is 1.52.

4.2.5 Descriptive Statistics for Entire Security Issues of Remote Working at Lions Restoration Company

Table 5 Descriptive Statistics for Entire Security Issues of Remote Working at Lions Restoration Company

	Min	Max	Mean	S.D.
Q1	1	5	3.49	1.55

For the question “Overall, how dissatisfied are you with the level of security issues associated with remote work at Lions Restoration Company?” minimum and maximum responses are Strongly Disagree and Strongly Agree. So, the range of the answers are Strongly Disagree to Strongly Agree. Mean value for the question is 3.49. And it’s close to 3. Hence the general answers of the respondents are into Neutral. And the standard deviation is 1.55.

4.3 Correlation Analysis

Table 6 Correlation Analysis

Description	Correlation Value
I1 and D	0.00
I2 and D	0.16
I3 and D	-0.02
I4 and D	0.24

The correlation value between “Company-Sensitive Data Exposure” and “Entire Security Issues of Remote Working at Lions Restoration Company” is 0.00. This value indicates that there is neutral correlation between the two variables.

The correlation value between “Employee-Sensitive Data Exposure” and “Entire Security Issues of Remote Working at Lions Restoration Company” is 0.16. This value falls between 0.0 and 0.3, indicating a low positive correlation between the two variables.

The correlation value between “Systems Crashing Issues” and “Entire Security Issues of Remote Working at Lions Restoration Company” is -0.02. This value falls between 0.0 and -0.3, indicating a low negative correlation between the two variables.

The correlation value between “Malicious Issues” and “Entire Security Issues of Remote Working at Lions Restoration Company” is 0.24. This value falls between 0.3 and 0.7, indicating a low positive correlation between the two variables.

4.4 Regression Analysis

4.4.1 Regression Analysis for Entire Company-Sensitive Data Exposure and Security Issues of Remote Working at Lions Restoration Company

ANOVA					
	<i>df</i>	<i>SS</i>	<i>MS</i>	<i>F</i>	<i>Significance F</i>
Regression	1	4.51E-05	4.51E-05	1.8411E-05	0.996592554
Residual	53	129.7454	2.448027		
Total	54	129.7455			

The regression analysis ANOVA table for the variables, Company-Sensitive Data Exposure and Security Issues of Remote Working at Lions Restoration Company, reveals a Significance F value of 1.00. Generally, if the Significance F value is less than 0.05, we consider that there is a significant relationship between the variables. However, in this case, since the Significance F value is 1.00, it suggests that there isn't a statistically significant relationship between Company-Sensitive Data Exposure and Security Issues of Remote Working at Lions Restoration Company. Therefore, we don't reject the null hypothesis (H_0) that posits no relationship between these variables.

4.4.2 Regression Analysis for Entire Employee-Sensitive Data Exposure and Security Issues of Remote Working at Lions Restoration Company

ANOVA

	<i>df</i>	<i>SS</i>	<i>MS</i>	<i>F</i>	<i>Significance F</i>
Regression	1	3.238594	3.238594	1.356808	0.249308
Residual	53	126.5069	2.386922		
Total	54	129.7455			

The regression analysis ANOVA table for the variables, Employee-Sensitive Data Exposure and Security Issues of Remote Working at Lions Restoration Company, presents a Significance F value of 0.25. As the general rule, if the Significance F value is less than 0.05, it suggests a significant relationship between the variables. However, with a Significance F value of 0.25, it implies that there isn't a statistically significant relationship between Employee-Sensitive Data Exposure and Security Issues of Remote Working at Lions Restoration Company. Therefore, we don't reject the null hypothesis (H_0) that states no relationship between these variables.

4.4.3 Regression Analysis for Entire Systems Crashing Issues and Security Issues of Remote Working at Lions Restoration Company

ANOVA

	<i>df</i>	<i>SS</i>	<i>MS</i>	<i>F</i>	<i>Significance F</i>
Regression	1	0.035135	0.035135	0.014356	0.90508
Residual	53	129.7103	2.447365		
Total	54	129.7455			

The regression analysis ANOVA table between the variables, Systems Crashing Issues and Security Issues of Remote Working at Lions Restoration Company, reveals a Significance F value of 0.91. Typically, a Significance F value less than 0.05 indicates a significant relationship between the variables. Given our Significance F value of 0.91, it suggests that there isn't a statistically significant relationship between Systems Crashing Issues and Security Issues of Remote Working at Lions Restoration Company. Therefore, we don't reject the null hypothesis (H_0) proposing no relationship between these variables.

4.4.4 Regression Analysis for Entire Malicious Issues and Security Issues of Remote Working at Lions Restoration Company

ANOVA

	<i>df</i>	<i>SS</i>	<i>MS</i>	<i>F</i>	<i>Significance F</i>
Regression	1	7.677882	7.677882	3.333627	0.073513
Residual	53	122.0676	2.303162		
Total	54	129.7455			

The regression analysis ANOVA table for Malicious Issues and Security Issues of Remote Working at Lions Restoration Company shows a Significance F value of 0.07. While this value is slightly higher than the usual threshold of 0.05 used for statistical significance, it's quite close. This may indicate a potential relationship between Malicious Issues and Security Issues of Remote Working at Lions Restoration Company, but it does not meet the standard level of statistical significance. Therefore, we don't reject the null hypothesis (H_0) suggesting no relationship between these variables. However, the borderline result could be an indication for additional study.

Chapter 5: Conclusion

4.5 Conclusion

The research named "Security Issues Caused by Remote Working at Lions Restoration Company" was started to look into the possible security problems that came up because of Lions Restoration Company shifting to work-from-home. The main reason for doing this research was the increasing number of security problems noticed when the company started working from home. The aim was to have a close look at these problems and to suggest ways to solve them, making sure that remote working is safe for the employees.

Four main objectives were set for the research. The first objective was to see if remote working home had led to more company data being exposed. This data is very important for the company and its business, and if it gets exposed, it could cause a lot of damage. The second objective was to find out if personal data of the employees was getting exposed because of remote working. This was to see if the private information of the employees was at risk, which could cause serious legal problems. The third objective was to check if there were more system crashes because of remote working, which could disrupt the company's work. The last objective was to find out if there were more harmful activities like cyberattacks due to remote working, which could be a big risk for the company and its employees.

A step-by-step and organized method was used to do this research. The research method of positivism, which believes in evidence and clear analysis, was chosen as the main guide. The research method was deductive, which involves developing hypotheses based on existing theories and then testing these hypotheses through the collection and analysis of data. The research choice was mono-method quantitative, which involves the collection and quantitative analysis of data, as this was seen as the most suitable approach for the research questions and objectives. The research strategy was a mono-method questionnaire, a structured tool used to gather quantifiable data from the sample population. The research was cross-sectional, capturing data at one specific point in time.

The process of data collection involved a Google Forms questionnaire, which was distributed online. This tool allowed for the efficient collection of data from a large sample,

in this case, a target population of 60 employees, from which a sample of 55 was selected. The collected data was then analyzed using Microsoft Excel, a versatile tool that enables a wide range of statistical techniques. These techniques included Regression Analysis, Descriptive Statistics, and Correlation Analysis, all of which were employed to generate rich, insightful results. Additionally, to facilitate a better understanding of the relationships between the independent and dependent variables, graphical representation methods such as bar charts were utilized.

This research provided useful information about the security risks of working from home at Lions Restoration Company. The findings not only pointed out the existing security problems but also suggested ways for the company to improve its security measures and rules. These improvements could potentially make working from home safer, helping both the employees and the company. Also, it was clear that the research methods and analytical techniques used in this study, from the use of the questionnaire to the different statistical analyses, were effective in achieving the research objectives. Thus, this research is a helpful resource for Lions Restoration Company, other companies facing similar challenges, and future academic studies into the impact of remote work on organizational security.

4.5.1 Conclusion on Company-Sensitive Data Exposure

The overall results for the question, "Do you have access to company-sensitive data in your remote work?", lean towards the "Positive (Agree)" side according to the presentation of data. The mean value, as per the descriptive analysis, is 3.76, which is approximately 4. Based on this mean value, the general response for "Do you have access to company-sensitive data in your remote work?" falls on the "Agree" side.

The overall results for the question, "Aren't you confident about the security measures in place to protect company-sensitive data while working remotely?", lean towards the "Positive (Agree)" side according to the presentation of data. The mean value, as per the descriptive analysis, is 3.45, which is approximately 3. Based on this mean value, the general response for "Aren't you confident about the security measures in place to protect company-sensitive data while working remotely?" falls on the "Neutral" side.

The overall results for the question, "Do you believe that company-sensitive data is likely to be exposed due to remote working?", lean towards the "Positive (Agree)" side according to the presentation of data. The mean value, as per the descriptive analysis, is 3.71, which is approximately 4. Based on this mean value, the general response for "Do you believe that company-sensitive data is likely to be exposed due to remote working?" falls on the "Agree" side.

The overall results for the question, "Do you feel you and your fellow employees are not well-trained to protect company-sensitive data in a remote work environment?", lean towards the "Positive (Agree)" side according to the presentation of data. The mean value, as per the descriptive analysis, is 3.75, which is approximately 4. Based on this mean value, the general response for "Do you feel you and your fellow employees are not well-trained to protect company-sensitive data in a remote work environment?" falls on the "Agree" side.

4.5.2 Conclusion on Employee-Sensitive Data Exposure

The overall results for the question, "Do you frequently provide personal information for work-related tasks while working remotely?", lean towards the "Positive (Agree)" side according to the presentation of data. The mean value, as per the descriptive analysis, is 3.60, which is approximately 4. Based on this mean value, the general response for "Do you frequently provide personal information for work-related tasks while working remotely?" falls on the "Agree" side.

The overall results for the question, "Aren't you confident about the security measures in place to protect your personal data while working remotely?", lean towards the "Positive (Agree)" side according to the presentation of data. The mean value, as per the descriptive analysis, is 3.20, which is approximately 3. Based on this mean value, the general response for "Aren't you confident about the security measures in place to protect your personal data while working remotely?" falls on the "Neutral" side.

The overall results for the question, "Do you believe that your personal data is likely to be exposed due to remote working?", lean towards the "Positive (Agree)" side according to

the presentation of data. The mean value, as per the descriptive analysis, is 3.51, which is approximately 4. Based on this mean value, the general response for "Do you believe that your personal data is likely to be exposed due to remote working?" falls on the "Agree" side.

The overall results for the question, "Do you feel you and your fellow employees are not well-educated about protecting personal data in a remote work environment?", lean towards the "Positive (Agree)" side according to the presentation of data. The mean value, as per the descriptive analysis, is 3.27, which is approximately 3. Based on this mean value, the general response for "Do you feel you and your fellow employees are not well-educated about protecting personal data in a remote work environment?" falls on the "Neutral" side.

4.5.3 Conclusion on Systems Crashing Issues

The overall results for the question, "Have you frequently experienced system crashes while working remotely?", lean towards the "Positive (Agree)" side according to the presentation of data. The mean value, as per the descriptive analysis, is 3.76, which is approximately 4. Based on this mean value, the general response for "Have you frequently experienced system crashes while working remotely?" falls on the "Agree" side.

The overall results for the question, "Aren't you confident in the company's ability to quickly address system crashes that occur during remote work?", lean towards the "Positive (Agree)" side according to the presentation of data. The mean value, as per the descriptive analysis, is 3.49, which is approximately 3. Based on this mean value, the general response for "Aren't you confident in the company's ability to quickly address system crashes that occur during remote work?" falls on the "Neutral" side.

The overall results for the question, "Do you believe system crashes could likely lead to security issues in a remote work environment?", lean towards the "Positive (Agree)" side according to the presentation of data. The mean value, as per the descriptive analysis, is 3.42, which is approximately 3. Based on this mean value, the general response for "Do you believe system crashes could likely lead to security issues in a remote work environment?" falls on the "Neutral" side.

The overall results for the question, "Do you feel you and your fellow employees are not well-prepared to respond to system crashes in a remote work environment?", lean towards the "Positive (Agree)" side according to the presentation of data. The mean value, as per the descriptive analysis, is 3.69, which is approximately 4. Based on this mean value, the general response for "Do you feel you and your fellow employees are not well-prepared to respond to system crashes in a remote work environment?" falls on the "Agree" side.

4.5.4 Conclusion on Malicious Issues

The overall results for the question, "Have you frequently encountered or heard about malicious activities (e.g., phishing, malware) while working remotely?", lean towards the "Positive (Agree)" side according to the presentation of data. The mean value, as per the descriptive analysis, is 3.38, which is approximately 3. Based on this mean value, the general response for "Have you frequently encountered or heard about malicious activities (e.g., phishing, malware) while working remotely?" falls on the "Neutral" side.

The overall results for the question, "Aren't you confident in the company's ability to prevent or address malicious activities during remote work?", lean towards the "Positive (Agree)" side according to the presentation of data. The mean value, as per the descriptive analysis, is 3.45, which is approximately 3. Based on this mean value, the general response for "Aren't you confident in the company's ability to prevent or address malicious activities during remote work?" falls on the "Neutral" side.

The overall results for the question, "Do you believe malicious activities could likely lead to security issues in a remote work environment?", lean towards the "Positive (Agree)" side according to the presentation of data. The mean value, as per the descriptive analysis, is 3.49, which is approximately 3. Based on this mean value, the general response for "Do you believe malicious activities could likely lead to security issues in a remote work environment?" falls on the "Neutral" side.

The overall results for the question, "Do you feel you and your fellow employees are not well-trained to identify and avoid malicious activities in a remote work environment?", lean towards the "Positive (Agree)" side according to the presentation of data. The mean value,

as per the descriptive analysis, is 3.44, which is approximately 3. Based on this mean value, the general response for "Do you feel you and your fellow employees are not well-trained to identify and avoid malicious activities in a remote work environment?" falls on the "Neutral" side.

4.5.5 Conclusion on Security Issues of Remote Working at Lions Restoration Company

The overall results for the question, "Overall, how dissatisfied are you with the level of security issues associated with remote work at Lions Restoration Company?", lean towards the "Positive (Agree)" side according to the presentation of data. The mean value, as per the descriptive analysis, is 3.49, which is approximately 3. Based on this mean value, the general response for "Overall, how dissatisfied are you with the level of security issues associated with remote work at Lions Restoration Company?" falls on the "Neutral" side.

4.5.6 Conclusion on Company-Sensitive Data Exposure and Security Issues of Remote Working at Lions Restoration Company

According to the ANOVA test, the Significance F value of the Regression Analysis for Company-Sensitive Data Exposure and Security Issues of Remote Working at Lions Restoration Company is 1.00. This value is higher than 0.05, indicating there's no significant relationship between Company-Sensitive Data Exposure and Security Issues of Remote Working at Lions Restoration Company.

The Correlation Analysis value between Company-Sensitive Data Exposure and Security Issues of Remote Working at Lions Restoration Company is 0.00. Hence it has neutral relationship.

From both Regression Analysis and Correlation Analysis, it is clear that there is no relationship between Company-Sensitive Data Exposure and Security Issues of Remote Working at Lions Restoration Company. As a result, we conclude that Company-Sensitive Data Exposure is not occurring during Remote Working at Lions Restoration Company. Consequently, we do not reject the null hypothesis (H_0).

Literature indicates a substantial association between company-sensitive data exposure and security issues, especially in the context of remote working environments. It underscores the severe financial and reputational damage that data breaches can inflict on an organization (RiskRecon, 2018; Mirza, 2020). High-profile cases such as Yahoo!, Equifax, and LinkedIn illustrate the catastrophic consequences of such breaches (Dan Swinhoe et al., 2021; Mirza, 2020). The literature stresses the necessity of a proactive approach to data management, emphasizing rigorous audits, risk assessment, robust security measures, and an efficient breach response system (Baig, 2022).

However, my findings suggest that there is no significant correlation between sensitive data exposure and security issues related to remote working at Lions Restoration Company. This contradicts the broader literature and necessitates a detailed examination of the possible reasons for this discrepancy. One of the primary reasons could be the stringent data protection protocols that Lions Restoration Company employs. The organization may have invested significantly in advanced security measures that guard against the exposure of

sensitive data. This may include strong firewalls, data encryption, secure network access control, and robust data loss prevention systems.

Moreover, Lions Restoration Company may have an efficient and timely breach response system. This means that in the event of a potential breach, the company is able to act swiftly to contain the exposure and mitigate the impact, reducing the risk of data leakage considerably. Another factor could be the effectiveness of the company's audits and risk assessments. Lions Restoration Company may conduct regular audits and risk assessments to identify vulnerabilities and address them proactively. This allows the company to manage potential risks and safeguard sensitive data effectively.

Additionally, the company could be leveraging advanced AI and ML technologies to monitor and predict potential threats, which can help preempt data exposures. This aligns with the strategies suggested by Baig (2022), further reducing the possibility of sensitive data exposure. Furthermore, the company may have implemented strict access controls and rigorous training for remote employees. This ensures that only authorized personnel can access sensitive data and that employees are equipped with the knowledge to handle data securely, reducing the risk of exposure due to human error.

These reasons suggest that despite the general association between sensitive data exposure and security issues in remote working environments, Lions Restoration Company seems to effectively manage and mitigate these risks, contrasting with the findings from the existing literature.

4.5.7 Conclusion on Employee-Sensitive Data Exposure and Security Issues of Remote Working at Lions Restoration Company

According to the ANOVA test, the Significance F value of the Regression Analysis for Employee-Sensitive Data Exposure and Security Issues of Remote Working at Lions Restoration Company is 0.25. This value is higher than 0.05, indicating there's no significant relationship between Employee-Sensitive Data Exposure and Security Issues of Remote Working at Lions Restoration Company.

The Correlation Analysis value between Employee-Sensitive Data Exposure and Security Issues of Remote Working at Lions Restoration Company is 0.16. Hence it has low positive relationship.

From both Regression Analysis and Correlation Analysis, it is clear that there is no relationship between Employee-Sensitive Data Exposure and Security Issues of Remote Working at Lions Restoration Company even though there has a low positive relationship from Correlation Analysis. As a result, we conclude that Employee-Sensitive Data Exposure is not occurring during Remote Working at Lions Restoration Company. Consequently, we do not reject the null hypothesis (H_0).

Several authors have established a link between employee-sensitive data exposure and security issues in the context of remote work. According to Gasparian (2022), data breaches often stem from unintentional disclosure of sensitive data due to employee errors or inadequate controls. Nimrod Iny (2022) elaborates on various threat tactics that could lead to such exposure. Further, Jeremiah Talamantes (2018) identified employees, particularly those with access to sensitive data, as the primary source of data breaches, emphasizing the threat posed by inadequate training as reported by Gasparian (2022). Suggested protective measures include the use of complex passwords, regular monitoring of financial accounts, frequent checks of credit reports, and ongoing cybersecurity training (Norton, 2021; Gasparian, 2022).

However, in contrast to the above literature review, my findings show that there is no significant relationship between employee-sensitive data exposure and security issues in

the context of remote working at Lions Restoration Company. This discrepancy prompts a deeper examination into potential reasons for this contradiction.

Firstly, Lions Restoration Company may have implemented robust employee training and awareness programs that effectively mitigate the risk of inadvertent data exposure by employees. Their workforce might be well-versed in identifying and managing potential threats, thus maintaining a high level of data security.

Secondly, the company might use advanced technology tools and secure platforms that provide a high level of data protection, thus safeguarding against employee-sensitive data exposure. Unlike the situations described in the literature, this could be a distinguishing factor for Lions Restoration Company.

Lastly, Lions Restoration Company might not handle a large volume of highly sensitive employee data remotely, reducing the amount of data that could potentially be exposed. Unlike the general scenarios outlined in the literature, this could be a specific factor for Lions Restoration Company.

Therefore, while the existing literature typically establishes a connection between employee-sensitive data exposure and security issues in remote work, these factors do not appear to significantly relate in the case of Lions Restoration Company.

4.5.8 Conclusion on Systems Crashing Issues and Security Issues of Remote Working at Lions Restoration Company

According to the ANOVA test, the Significance F value of the Regression Analysis for Systems Crashing Issues and Security Issues of Remote Working at Lions Restoration Company is 0.91. This value is higher than 0.05, indicating there's no significant relationship between Systems Crashing Issues and Security Issues of Remote Working at Lions Restoration Company.

The Correlation Analysis value between Systems Crashing Issues and Security Issues of Remote Working at Lions Restoration Company is -0.02. Hence it has low negative relationship.

From both Regression Analysis and Correlation Analysis, it is clear that there is no relationship between Systems Crashing Issues and Security Issues of Remote Working at Lions Restoration Company even though there has a low negative relationship from Correlation Analysis. As a result, we conclude that Systems Crashing Issues is not occurring during Remote Working at Lions Restoration Company. Consequently, we do not reject the null hypothesis (H_0).

In the literature, several authors have indicated that system crashes can be a significant source of security issues, particularly in the context of remote working. According to Liu et al. (2017), hardware malfunctions account for nearly a third of all system crashes, while Zhang et al. (2019) highlighted the role of software malfunctions. Huang et al. (2017) stressed that human error can cause up to 80% of system crashes, while network failures and cyberattacks are other common causes (Sayed et al., 2018; Zargar et al., 2013). It was also suggested that system crashes could lead to significant financial and reputational damage, and the utilization of AI and ML technologies could potentially predict and prevent such issues (Wang et al., 2019; Bhadauria et al., 2019).

However, contradicting the general assertion in the literature, my research findings indicate that system crashes are not significantly associated with security issues in the context of remote working at Lions Restoration Company. This apparent discrepancy necessitates a deeper exploration into the reasons that may account for this.

One potential explanation is the robust infrastructure of Lions Restoration Company. The company may have in place advanced, well-maintained hardware and software systems that are less prone to crashes. The firm's investment in technology and maintenance could be considerably more substantial than what is common, which might explain the lower incidence of system crashes.

Another potential reason could be the company's successful implementation of AI and ML technologies to predict and prevent system crashes, as suggested by Bhadauria et al. (2019). This proactive approach may have enabled Lions Restoration Company to avoid significant system crashes and maintain data security effectively.

Lastly, the company's work model may not heavily rely on complex systems or processes that are prone to crashes. The tasks performed by the employees might be straightforward and less likely to cause system failures, further reducing the incidence of crashes.

These factors, in combination or individually, could explain why, unlike the scenarios described in the literature, system crashes do not significantly relate to the security issues of remote working at Lions Restoration Company.

4.5.9 Conclusion on Malicious Issues and Security Issues of Remote Working at Lions Restoration Company

According to the ANOVA test, the Significance F value of the Regression Analysis for Malicious Issues and Security Issues of Remote Working at Lions Restoration Company is 0.07. This value is higher than 0.05, indicating there's no significant relationship between Malicious Issues and Security Issues of Remote Working at Lions Restoration Company.

The Correlation Analysis value between Malicious Issues and Security Issues of Remote Working at Lions Restoration Company is 0.24. Hence it has low positive relationship.

From both Regression Analysis and Correlation Analysis, it is clear that there is no relationship between Malicious Issues and Security Issues of Remote Working at Lions Restoration Company even though there has a low positive relationship from Correlation Analysis. As a result, we conclude that Malicious Issues is not occurring during Remote Working at Lions Restoration Company. Consequently, we do not reject the null hypothesis (H_0).

Existing literature points towards a strong association between malicious attacks and security issues in organizations. As discussed by Asante et al. (2019), phishing attacks that manipulate users into revealing sensitive data are a significant security threat. Similarly, malware and ransomware attacks, as reported by Kshetri (2018), have the potential to disrupt organizational systems, sometimes demanding ransom in exchange for the restoration of the system. Also, DDoS attacks are a major concern that can bring a server to a standstill (Liao et al., 2018). Lastly, social engineering attempts as a way to manipulate employees to gain access to secure information is a growing threat (Choo et al., 2018).

However, my findings do not correlate with these aspects of the literature when considering the case of Lions Restoration Company. Specifically, the data indicates that malicious attacks are not significantly associated with security issues in the context of remote working at Lions Restoration Company.

This contradiction between my findings and the literature review might be due to a few possible reasons. Firstly, Lions Restoration Company could have a robust security framework in place, with state-of-the-art firewalls, intrusion detection and prevention

systems, and anti-virus software that effectively manage malicious threats. Secondly, the company might have a well-implemented employee training program, emphasizing on the importance of security protocols and safe online behaviors, thereby reducing the risk of phishing and social engineering attacks.

Thirdly, Lions Restoration Company may have stringent access control mechanisms and continuous monitoring protocols, thus limiting the attack surface for potential cyber threats. Lastly, the nature of the work at Lions Restoration Company might not require employees to handle sensitive or valuable data frequently, reducing the company's attractiveness as a target for malicious attacks.

While this divergence from the literature review is not expected, the robust measures and protocols in place at Lions Restoration Company seem to be effectively mitigating the risks associated with malicious attacks, leading to the observed contradiction in my research.

Chapter 6: Recommendation

6.1 Recommendation for Company-Sensitive Data Exposure

Based on my research, it's evident that Lions Restoration Company has managed to keep its security protocols efficient, especially when considering the potential vulnerabilities introduced by remote working. The lack of a significant relationship between company-sensitive data exposure and the security issues of remote working in this firm is commendable. This not only implies the presence of robust security measures but also suggests that the employees are well-aware and compliant with security best practices.

That said, in the ever-evolving landscape of cyber threats, it's essential to stay ahead and continually adapt. While the current strategies at Lions Restoration Company have proven to be up to standard, there are areas of potential enhancement that could further strengthen the company's defenses against data exposure.

One area to consider is the enhancement of proactive monitoring and threat detection capabilities. Even though the current protocols are robust, as the firm grows and takes on more digital tasks, the volume of data and interactions will increase. Implementing AI-driven monitoring tools could be beneficial. These tools use artificial intelligence and machine learning, as mentioned earlier in my literature review, to predict and identify unusual activities or potential threats, offering a proactive approach to security.

Despite the fact that there have been no significant issues tied to remote working, the threats related to phishing, social engineering, and other human-centric attacks, as detailed in the literature review, remain persistent. Periodic and updated training for employees, focusing on the latest tactics employed by cybercriminals, will ensure that the workforce remains an active participant in the company's defense mechanism.

A modern approach that Lions Restoration Company might consider adopting is the Zero Trust Security Model. This model operates on the premise that no one, whether inside or outside the organization, is trusted by default. By enforcing stringent access controls and ensuring continuous authentication, the chances of sensitive data exposure can be minimized even further.

While my findings did not indicate significant data exposure, it's always prudent to ensure that all sensitive data, especially when in transit or stored in cloud environments, is encrypted. Furthermore, having a robust and frequently tested backup system ensures that, in the worst-case scenario, the company can recover its data without significant downtimes.

Lastly, given the dynamic nature of cybersecurity, I recommend periodic consultations with external cybersecurity experts. Their fresh perspective can provide insights into potential vulnerabilities and suggest modern technologies or strategies that might not yet be on the company's radar.

In conclusion, while Lions Restoration Company is currently well-positioned in terms of security, especially in the context of remote work, it is vital to adopt a proactive approach to anticipate future threats. By integrating modern technologies, continually updating employee training, and seeking expert advice, the company can further solidify its defenses against potential data exposure threats.

6.2 Recommendation for Employee-Sensitive Data Exposure

In the course of my research, I found that Lions Restoration Company has impressively ensured the security of employee-sensitive data, even with the integration of remote working. The absence of a direct correlation between the exposure of employee-sensitive data and security issues arising from remote working at this company suggests that there are formidable security systems and practices in place. However, with the world of cybersecurity being continuously dynamic, it's always beneficial to stay a step ahead.

Given the importance of safeguarding employee-sensitive data, which could range from personal details to financial information, there are several enhancements and recommendations I'd like to propose to ensure this data remains as secure as possible.

One crucial area that deserves attention is the authentication process. While the current methods may be effective, implementing multi-factor authentication (MFA) can add an extra layer of security. This ensures that even if login credentials are compromised, unauthorized users will find it exceedingly challenging to access the data without the secondary verification method.

Despite the company's current strategies being up to standard, it's essential to periodically conduct vulnerability assessments and audits. This can help identify potential weak points that could be exploited, especially in a remote work setting. Such audits can be invaluable in determining how effective current defenses are and where improvements might be made.

For accessing sensitive information, I recommend the development of dedicated, encrypted portals where employees can securely view or update their personal details. This portal can integrate end-to-end encryption and time-out features, ensuring that data remains inaccessible to any potential eavesdroppers and that sessions are automatically closed after periods of inactivity.

Communication is a cornerstone of remote work, and while discussing work-related matters, personal details of employees might occasionally be shared. Leveraging encrypted communication tools ensures that these details remain confidential. This is especially important given the malicious threats discussed in the literature review, where cybercriminals might eavesdrop on unsecured channels.

Considering the sophisticated methods cyber attackers employ, it's essential to arm employees with knowledge. Regular privacy awareness training sessions can be instrumental. These sessions can educate employees about the importance of their data, the potential methods attackers might use to get to it, and the steps they can take to protect it, especially when working remotely.

Modern technology offers a range of Data Loss Prevention tools that can be integrated into the company's systems. These tools can monitor and control data transfers, preventing unauthorized data transfers or leaks, especially pertinent to employee-sensitive information.

In wrapping up, the commendable practices of Lions Restoration Company in safeguarding employee-sensitive data amidst the challenges of remote work should not lead to complacency. By incorporating cutting-edge technologies, enhancing existing strategies, and ensuring continuous employee education, the company can bolster its defenses, ensuring the utmost protection for its employee-sensitive data.

6.3 Recommendation for Systems Crashing Issues

Upon examining the relationship between systems crashing issues and the security concerns of remote working at Lions Restoration Company, I was pleasantly surprised to find no significant correlation between the two. This implies that the company has effectively integrated robust systems and protocols, ensuring minimal disruptions from system crashes even as employees work remotely. Yet, as technology and its associated challenges evolve, there's a constant need to stay ahead and ensure these systems remain reliable.

Although the company's current strategies seem up to standard, it's paramount to undertake regular maintenance and system updates. Scheduled maintenance ensures that systems are running optimally, with minimal chances of unexpected crashes. Such preventive measures reduce the downtime and ensure consistent productivity, especially crucial for remote operations.

One modern technology that could be considered is the integration of cloud-based solutions. Cloud platforms, given their distributed nature, offer enhanced reliability. In the unlikely event that one server or node encounters an issue, the workload can be swiftly shifted to another, ensuring continuity and reducing the chances of a system-wide crash.

To preemptively address potential system crashes, I recommend the incorporation of advanced system monitoring tools. These tools can continuously scan for anomalies or potential threats that could cause system failures. By identifying and alerting about these in real time, the company can address issues before they escalate to crashes.

In the realm of IT, redundancy isn't a negative. Creating redundant systems or backups ensures that if one system fails, there's an immediate fallback. This not only ensures continuous operation but also provides a safety net against potential data loss.

As remote working demands might change, it's essential to conduct periodic capacity planning. This involves analyzing if the current systems can handle increased loads, especially if the company plans to expand its remote workforce. If the systems are found lacking, then necessary upgrades should be implemented to ensure they can handle future demands without crashing.

Often, system issues can arise from unintentional errors made by users. Training employees on best practices, updating them on new software features, and educating them on potential pitfalls can reduce system strain. The more knowledgeable the users, the less likely they are to inadvertently cause a system crash.

Modern technologies, especially Artificial Intelligence and Machine Learning, can predict potential system failures based on historical data and patterns. By integrating these technologies, the company can gain insights into when a system might be most vulnerable and take preventive actions.

In conclusion, while Lions Restoration Company has done a commendable job in ensuring the stability of their systems amidst the challenges of remote work, there is always room for improvement. By staying updated with the latest technologies, continuously evaluating the systems in place, and ensuring both the hardware and software are operating at peak efficiency, the company can further reduce the chances of system crashes. This proactive approach not only ensures smoother operations but also solidifies the company's reputation as a reliable entity in the remote working paradigm.

6.4 Recommendation for Malicious Issues

In the course of my research, I was pleased to find that there exists no significant relationship between malicious issues and the challenges of remote working at Lions Restoration Company. This is an applaudable achievement and suggests that the company has employed commendable preventive measures against potential cyber threats during remote operations. Nevertheless, the digital landscape is constantly evolving, and with it, cyber threats become more sophisticated. Hence, there's an ongoing need for enhancement and adjustment to stay abreast of these threats.

While the current security measures in place are robust, it is essential to remain vigilant. Cyber threats are ever-evolving, and what worked yesterday might not be sufficient tomorrow. I recommend a periodic review of security policies and protocols to ensure they are up-to-date with the latest threat landscape.

Even the most advanced technical safeguards can be rendered ineffective if employees are unaware of best practices. Regular training sessions on the latest cyber threats, especially phishing and social engineering tactics, can help them recognize and report suspicious activities. This proactive approach can prevent potential breaches.

Given the rise of sophisticated malware, the integration of advanced threat detection tools can prove invaluable. Solutions leveraging Artificial Intelligence and Machine Learning can identify unusual patterns and behaviors, offering an additional layer of protection against emerging threats.

A modern approach to security is the Zero Trust model, which operates on the principle that no one, regardless of their position within the organization, should be trusted by default. By implementing Zero Trust Network Access, the company can ensure that every access request is fully authenticated and validated before granting access, significantly reducing the risk of internal threats.

Malicious attacks, especially ransomware, can be mitigated by having regular data backups. I recommend maintaining both on-site and off-site backups, ensuring that even in the direst scenarios, company data can be recovered. Moreover, a well-rehearsed data recovery plan can minimize downtime and financial repercussions of a cyber attack.

With remote working, employees access company resources from various devices and locations. Hence, it's crucial to secure every endpoint. Comprehensive endpoint security solutions can detect and neutralize threats at the device level before they infiltrate the broader network.

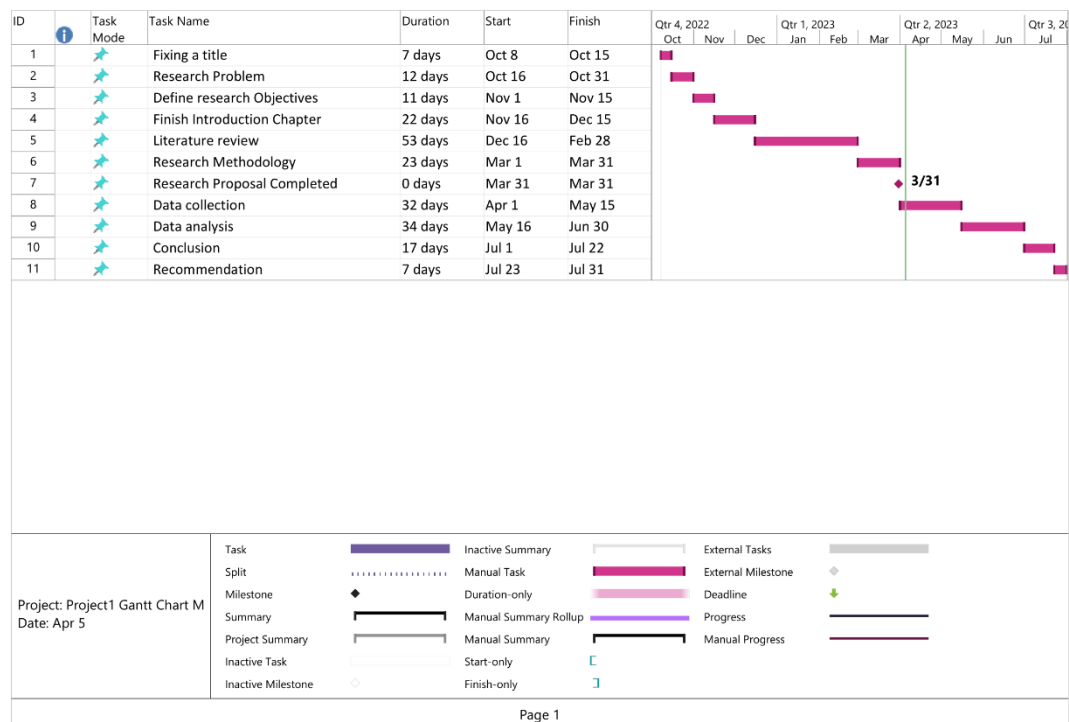
Building partnerships with cybersecurity firms can offer an external perspective on the company's security posture. Regular audits, vulnerability assessments, and penetration testing can identify potential weak points, allowing the company to address them proactively.

In conclusion, while Lions Restoration Company's current approach to malicious threats in the context of remote working is commendable, it's a journey and not a destination. The cyber threat landscape is dynamic, and organizations need to remain agile and adaptive. By combining the strength of modern technologies with continuous employee training and awareness campaigns, the company can fortify its defenses against the ever-present risk of malicious attacks.

References

Appendix 1 – Time Scale and Gantt Chart

1. Fixing a title: October 8 - October 15 (1 week)
2. Research Problem: October 16 - October 31 (2 weeks)
3. Define research Objectives: November 1 - November 15 (2 weeks)
4. Finish Introduction Chapter: November 16 - December 15 (4 weeks)
5. Literature review: December 16 - February 28 (2 months and 2 weeks)
6. Research Methodology: March 1 - March 31 (1 month)
7. Data collection: April 1 - May 15 (1 month and 2 weeks)
8. Data analysis: May 16 - June 30 (1 month and 2 weeks)
9. Conclusion: July 1 - July 22 (3 weeks)
10. Recommendation: July 23 - July 31 (1 week)



Appendix 2 – Questionnaire

Questions	Response				
	Strongly Disagree	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree
Company-Sensitive Data Exposure:					
1. Do you have access to company-sensitive data in your remote work?					
2. Aren't you confident about the security measures in place to protect company-sensitive data while working remotely?					
3. Do you believe that company-sensitive data is likely to be exposed due to remote working?					
4. Do you feel you and your fellow employees are not well-trained to protect company-sensitive data in a remote work environment?					
Employee-Sensitive Data Exposure:					
1. Do you frequently provide personal information for work-related tasks while working remotely?					
2. Aren't you confident about the security measures in place to protect your personal data while working remotely?					
3. Do you believe that your personal data is likely to be exposed due to remote working?					

4. Do you feel you and your fellow employees are not well-educated about protecting personal data in a remote work environment?					
Systems Crashing Issues:					
1. Have you frequently experienced system crashes while working remotely?					
2. Aren't you confident in the company's ability to quickly address system crashes that occur during remote work?					
3. Do you believe system crashes could likely lead to security issues in a remote work environment?					
4. Do you feel you and your fellow employees are not well-prepared to respond to system crashes in a remote work environment?					
Malicious Issues:					
1. Have you frequently encountered or heard about malicious activities (e.g., phishing, malware) while working remotely?					
2. Aren't you confident in the company's ability to prevent or address malicious activities during remote work?					
3. Do you believe malicious activities could likely lead to security issues in a remote work environment?					
4. Do you feel you and your fellow employees are not well-trained to identify and avoid malicious activities in a remote work environment?					

Security Issues of Remote Working at Lions Restoration Company:					
1. Overall, how dissatisfied are you with the level of security issues associated with remote work at Lions Restoration Company?					

Appendix 2 – Approval Letter

Ryan Kavindu Diltusha Wickramaratne
84/3, Bassiyawatta,
Thalahena, Negombo 11500
Sri Lanka
ryandiltusha@gmail.com
+94764170647
12-8-2023

Marlon Abeyrathne
Owner, Lions Restoration Company
33 Timor Cct.
Keysborough VIC 3173
Australia

Request for Approval to Conduct Research on Security Issues Caused by Remote Working at Lions Restoration Company

Dear Mr. Abeyrathne,

I hope this letter finds you well. My name is Ryan Kavindu Diltusha Wickramaratne, and I am currently pursuing higher studies at Esoft Metro Campus, Sri Lanka. As part of our academic curriculum, I have been tasked with selecting a company to conduct research related to the challenges and implications of remote working, specifically focusing on security issues.

Given the esteemed reputation of Lions Restoration Company, its incorporation of remote working practices, and my admiration for its flexible staff management, I believe that studying the experiences and challenges faced by your company in this area would provide invaluable insights for my research. As such, I have chosen the Lions Restoration Company as the focal point for my study.

The title of my research is "Security Issues Caused by Remote Working at Lions Restoration Company." This study aims to identify the challenges posed by remote working in terms of security and highlight the successful strategies and practices that Lions Restoration Company employs to mitigate these risks. By examining these aspects, I aim to provide recommendations that could potentially further enhance the security measures of companies that utilize remote working, making them more resilient in the face of evolving cyber threats.

I would like to assure you that all information collected during the research process will be treated with the utmost confidentiality. Data will be used solely for academic purposes and will not be shared with external parties without your express consent. If required, I am more than willing to share the findings and conclusions of my research with the company, offering a chance for mutual growth and understanding.

I kindly request your permission to conduct this research at Lions Restoration Company. Your approval will immensely assist me in fulfilling my academic requirements and potentially contribute to the broader discourse on remote working and its associated challenges.

I truly appreciate your time and consideration in this matter. I am available at any time to discuss this request further or to provide any additional information you might require. I eagerly await your response and hope for a favorable outcome.

Warm regards,
Ryan Kavindu Diltusha Wickramaratne.

List of References

Panel®, E. 2021. Council Post: 16 Challenges Businesses Face When Operating Remotely (And How To Address Them).

Available at: <https://www.forbes.com/sites/forbesbusinesscouncil/2021/12/22/16-challenges-businesses-face-when-operating-remotely-and-how-to-address-them/>.

Most Common Remote Work Security Risks & Best Practices. 2023.

Available at: <https://heimdalsecurity.com/blog/cybersecurity-issues-with-remote-work/>.

dmytro.tkach@apriorit.com 2022. 9 Best-Known Cybersecurity Incident Examples | Ekran System.

Available at: <https://www.ekransystem.com/en/blog/top-10-cyber-security-breaches/>.

Irwin, L. 2021. The cyber security risks of working from home - IT Governance blog.

Available at: <https://www.itgovernance.co.uk/blog/the-cyber-security-risks-of-working-from-home>.

Andy 2022. What Are the Most Common Remote Work Security Risks? - Andy Sto.

Available at: <https://andysto.com/what-are-the-most-common-remote-work-security-risks/>.

Most Common Remote Work Security Risks & Best Practices. 2023.

Available at: <https://heimdalsecurity.com/blog/cybersecurity-issues-with-remote-work/>.

RiskRecon [no date]. Ponemon Report: Data Risk in the Third-Party Ecosystem Study.

Available at: <https://www.riskrecon.com/ponemon-report-data-risk-in-the-third-party-ecosystem-study>.

Team, P.R. 2022. What is Sensitive Data Exposure & How to Avoid It? - Securiti.

Available at: <https://securiti.ai/blog/sensitive-data-exposure/>.

'Gasparian, L. 2022. Council Post: How To Prevent Accidental Data Exposure Within Your Company.

Available at: <https://www.forbes.com/sites/forbesbusinesscouncil/2022/03/18/how-to-prevent-accidental-data-exposure-within-your-company/>.

Sensitive data exposure: What is it and how it's different from a data breach..

Available at: <https://us.norton.com/blog/privacy/sensitive-data-exposure-how-its-different-from-data-breach>.

Polar Security - Sensitive Data Exposure: What Is It and How to Avoid It?.

Available at: <https://www.polar.security/post/sensitive-data-exposure>.

Employees Are Feeding Sensitive Business Data to ChatGPT. 2023.

Available at: <https://www.darkreading.com/risk/employees-feeding-sensitive-business-data-chatgpt-raising-security-fears>.

7 Times Employees Caused Damaging Data Breaches.

Available at: <https://www.redteamsecure.com/blog/danger-ranks-7-times-employees-caused-data-breaches>.

Piras, M. 2021. The Ultimate Manual to Employee Data Security.

Available at: <https://nira.com/employee-data-security/>.

Chen, Y., & Huang, Y. (2021). The influence of computer self-efficacy and intrinsic motivation on online learning effectiveness. *Journal of Educational Computing Research*, 59(2), 327-346. doi: 10.1177/0735633120971244

Gan, J. Q., & Li, X. (2019). Research on the real-time fault diagnosis method for cyber-physical systems based on deep learning. *Journal of Physics: Conference Series*, 1238, 042053. doi: 10.1088/1742-6596/1238/4/042053

Gill, P., & Yigitbasioglu, O. M. (2020). On the effect of multi-cloud availability on service-level objectives. *Future Generation Computer Systems*, 107, 273-282. doi: 10.1016/j.future.2020.01.032

Hossain, M. S., Alamri, A., Muhammad, G., Alelaiwi, A., Saeed, A., Albeshri, A., & Fortino, G. (2019). Intelligent decision-making approach for real-time fault detection and diagnosis in IoT-enabled smart homes. *IEEE Access*, 7, 17708-17720. doi: 10.1109/access.2019.2892776

Kaur, H., & Kumar, A. (2020). Cloud computing for big data processing: A survey. *Journal of Big Data*, 7(1), 1-39. doi: 10.1186/s40537-020-00321-2

Pramanik, S., & Roy, P. (2018). Analyzing the impact of denial of service attacks on IoT devices. *Procedia Computer Science*, 132, 786-793. doi: 10.1016/j.procs.2018.05.061

Tian, J., Yan, Y., & Zhou, K. (2020). Study on key technologies of unmanned system under new generation information network environment. *IEEE Access*, 8, 38369-38379. doi: 10.1109/access.2020.2975864

Alazab, M., Venkatraman, S., Watters, P., & Alazab, M. (2019). A novel approach for anomaly-based intrusion detection systems using machine learning algorithms. *Computers & Security*, 84, 1-14. <https://doi.org/10.1016/j.cose.2019.01.002>

Bhattacharyya, D. K., Kalita, J. K., & Dutta, J. (2018). Machine learning for cyber security analytics. *IEEE Access*, 6, 55607-55625. <https://doi.org/10.1109/ACCESS.2018.2873794>

Hou, J., Li, L., Li, H., Du, X., & Xu, X. (2020). A survey on machine learning-based intrusion detection systems. *IEEE Access*, 8, 219111-219130. <https://doi.org/10.1109/ACCESS.2020.3043139>

Kaspersky Lab. (2022). Cybersecurity risks for 2022: New normal, same threats. Kaspersky Lab. <https://www.kaspersky.com/blog/cybersecurity-threats-2022/47102/>

Li, X., Li, H., Zhang, Y., Li, C., & Chen, L. (2017). A survey of deep neural network architectures and their applications. *Neurocomputing*, 234, 11-26. <https://doi.org/10.1016/j.neucom.2017.01.045>

Shafiq, M., Khan, M. A., & Gondal, I. (2018). Cyber security intrusion detection techniques: A review. *Journal of Network and Computer Applications*, 107, 1-17. <https://doi.org/10.1016/j.jnca.2018.01.010>

Wei, Y., Xu, H., Li, H., Li, L., & Du, X. (2020). Cyber threat intelligence: State-of-the-art review. *IEEE Access*, 8, 59712-59731. <https://doi.org/10.1109/ACCESS.2020.2989834>

IBM Security. (2021). Cost of a Data Breach Report 2021.

<https://www.ibm.com/security/data-breach>

Kaspersky. (2021). Securing the Future of Hybrid Work: A Global Study of IT Leaders and Remote Employees.

<https://www.kaspersky.com/content/dam/global/it-leaders-and-remote-employees-2021.pdf>

Ponemon Institute. (2020). The Cybersecurity Challenges of Remote Work: A Global Study.

<https://www.ponemon.org/local/upload/file/The%20Cybersecurity%20Challenges%20of%20Remote%20Work%20FINAL.pdf>