Higher Nationals

Internal verification of assessment decisions – BTEC (RQF)

INTERNAL VERIFICATION – ASSESSMENT DECISIONS			
Programme title	HND in Computing		
Assessor	Mr. Lilanka	**Internal Verifier**	
Unit(s)	Unit 13: Computing Research Project		
Assignment title	Final Research Project Proposal		
Student'sname	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 (ifrequired)		**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:

LO1 Examine appropriate research methodologies and approaches as part of the research process

Pass, Merit & Distinction Descripts	P1	□	P2	□	M1	□	D1	□

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			
Assessor signature		**Date**	
Student signature	ryandilthusha@gmail.com	**Date**	

Pearson
Higher Nationals in
Computing

Unit 13: Computing Research Project

Project Proposal

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 be sure to fill the details correctly.
2. This entire brief should be attached in first before you start answering.
3. All the assignments should prepare using word processing software.
4. All the assignments should print in A4 sized paper, and make sure to only use one side printing.
5. Allow 1" margin on each side of the paper. But on the left side you will need to leave room for binging.

Word Processing Rules

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

Important Points:

1. Check carefully the hand in date and the instructions given with the assignment. Late submissions will not be accepted.
2. Ensure that you give yourself enough time to complete the assignment by the due date.
3. Don't leave things such as printing to the last minute – excuses of this nature will not be accepted for failure to hand in the work on time.
4. You must take responsibility for managing your own time effectively.
5. 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.
6. Failure to achieve at least a PASS grade will result in a REFERRAL grade being given.
7. Non-submission of work without valid reasons will lead to an automatic REFERRAL. You will then be asked to complete an alternative assignment.
8. Take great care that if you use other people's work or ideas in your assignment, you properly reference them, using the HARVARD referencing system, in you text and any bibliography, otherwise you may be guilty of plagiarism.
9. If you are caught plagiarising you could have your grade reduced to A REFERRAL or at worst you could be excluded 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 way. 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 the Edexcel UK.
3. I know what the consequences will be if I plagiaries 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 aspects 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 Edexcel UK.
6. I understand that my assignment will not be considered as submitted if this document is not attached to the attached.

ryandilthusha@gmail.com

12/08/2023

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

Date:
(*Provide Submission Date*)

Assignment Brief

Student Name /ID Number	Ryan Wickramaratne (COL 00081762)
Unit Number and Title	Unit 13 – Computing Research Project
Academic Year	2020/2021
Unit Tutor	Mr. Lilanka
Assignment Title	**Final Research Project Proposal**
Issue Date	
Submission Date	
IV Name & Date	

Submission Format:

Research Project Proposal

- 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
- Reference using the Harvard referencing system.
- Please provide a referencing list using the Harvard referencing system.
- The recommended word limit is minimum 2000 words.

Unit Learning Outcomes:

LO1. Examine appropriate research methodologies and approaches as part of the research process.

Assignment Brief and Guidance:

Internet of Things

The Internet of Things (IoT) is the term which refers to the ever-growing network of physical objects with embedded sensors which can connect together via the internet allowing communication to occur between these objects and many other Internet-enabled devices and systems.

The IoT is quickly becoming a necessary aspect of people's daily lives. Physical items can now sense and collect data which can be controlled through digital and smart technology. The IoT extends internet connectivity beyond traditional devices like desktop and laptop computers, smartphones, and tablets to a diverse range of devices that can utilise embedded technology such as security systems, thermostats, cars, electronic appliances, lights, medical equipment etc. These devices, often called "connected" or "smart" devices, which can talk to other related devices (machine-to-machine (M2M) communication) and act on the information they get from one another. Along with the many benefits, there is also considerable concern over the IoT which must be overcome in order to harness the power of this free flow of information.

Research objective/question

Students are allowed to choose their own research topic for this unit. A central skill in selecting a research objective is the ability to select a suitable and focused research objective. One of the best ways to do this is to put it in the form of a question.

The range of topics to be selected could cover the following:

1. Underpinning security and privacy issues and resolutions: data mining, data processing (e.g. GDPR), encryption (e.g. blockchain)
2. Smart homes, smart buildings, and smart cities etc. and their impact on individuals and society.
3. The future of IoT e.g. automate manufacturing, medicine and healthcare, virtual world, AI, machine learning etc.
4. The IT infrastructure required to support IoT e.g., 5G, proliferation of sensors, interoperability

Consider that the development of a methodical and valid research proposal as the foundation for the project. Choose a topic of personal interest in a specialism and the topic chosen should allow a sufficient and suitable degree of research through the existence of adequate background materials.

The Learner requires to produce a research proposal that clearly defines a research question or hypothesis, supported by a literature review (Use the project proposal and ethical consideration form template formats)

1. Define the research problem or question. (This can be stated as a research question, objectives, or hypothesis).
2. Provide a literature review by giving the background and conceptualisation of your proposed area of study. (This would provide existing knowledge and benchmarks by which your data can be judged).
3. Consider and define the research methodology and research process. Demonstrate understanding of the pitfalls and limitations of the methods chosen and ethical issues that might arise.
4. Draw points (1–3, above) together into a research proposal for agreement with your tutor.

Grading Rubric

Grading Criteria	**Achieved**	**Feedback**
LO1 **Examine appropriate research methodologies and approaches as part of the research process.**		
P1 Produce a research proposal that clearly defines a research question or hypothesis, supported by a literature review		
P2 Examine appropriate research methods and conduct primary and secondary research.		
M1 Evaluate different research approaches and methodology and make justifications for the choice of methods selected based on philosophical/ theoretical frameworks.		
D1 Critically evaluate research methodologies and processes in application to a computing research project to justify chosen research methods and analysis.		

Research Proposal Form

Student Name	Ryan Wickramaratne (COL 00081762)		
Student number	E107784	**Date**	
Centre Name	Bambalapitiya Esoft		
Unit	13		
Tutor	Mr. Lilanka		
Proposed title			
Security issues caused by Remote Working at Lions Restoration			

Section One: Title, objective, responsibilities
Title or working title of research project (in the form of a question, objective or hypothesis): Research project objectives (e.g. what is the question you want to answer? What do you want to learn how to do? What do you want to find out?): Introduction, Objective, Sub Objective(s), Research Questions and/or Hypothesis

Section Two: Reasons for choosing this research project
Reasons for choosing the project (e.g. links to other subjects you are studying, personal interest, future plans, knowledge/skills you want to improve, why the topic is important): Motivation, Research gap

Section Three: Literature sources searched
Use of key literature sources to support your objective, Sub Objective, research question and/or hypothesis: Can include the Conceptual Framework

Section Four: Activities and timescales	
Activities to be carried out during the research project (e.g. research, development, analysis of ideas, writing, data collection, numerical analysis, tutor meetings, production of final outcome, evaluation, writing the report) and How long this will take:	
Milestone	**Propose completion data**

Section Five: Research approach and methodologies
Type of research approach and methodologies you are likely to use, and reasons for your choice: What your areas of research will cover: Research Onion; Sample Strategy/Method; Sample Size

Reference List

Comments and agreement from tutor					
Comments (optional):					
I confirm that the project is not work which has been or will be submitted for another qualification and is appropriate.					
Agreed	Yes ☐ No ☐	Name		Date	

Comments and agreement from project proposal checker (if applicable)	
Comments (optional):	
I confirm that the project is appropriate.	

Agreed	Yes ☐ No ☐	Name		Date	

Research Ethics Approval Form

All students conducting research activity that involves human participants or the use of data collected from human participants are required to gain ethical approval before commencing their research. Please answer all relevant questions and note that your form may be returned if incomplete.

Section 1: Basic Details	
Project title:	Security issues caused by Remote Working at Lions Restoration
Student name:	Ryan Wickramaratne (COL 00081762)
Student ID number:	E107784
Programme:	Computing Research Project Project Proposal
School:	Bambalapitiya Esoft
Intended research start date:	
Intended research end date:	

Section 2: Project Summary

Please select all research methods that you plan to use as part of your project

- Interviews: ☐
- Questionnaires: ☒
- Observations: ☐
- Use of Personal Records: ☐
- Data Analysis: ☐
- Action Research: ☐
- Focus Groups: ☐
- Other (please specify): ☐ ....

Section 3: Participants

Please answer the following questions, giving full details where necessary.

Will your research involve human participants? Yes ☑

Who are the participants? Tick all that apply:

Age 12-16 ☐ Young People aged 17–18 ☐ Adults ☒

How will participants be recruited (identified and approached)?

- Participants will be recruited from the employees currently engaged in remote work at Lions Restoration.

Describe the processes you will use to inform participants about what you are doing:

- Sending an email to all employees who work remotely, inviting them to participate in the study. The email will contain detailed information about the study's purpose, the processes involved, the voluntary nature of their participation, and the measures taken to ensure their privacy and confidentiality.

Studies involving questionnaires:

Will participants be given the option of omitting questions they do not wish to answer?

Yes ☐ No ☒

If **"NO"** please explain why below and ensure that you cover any ethical issues arising from this.

- In this study, it's preferable for participants to answer all the questions to ensure the collected data is consistent and comparable across participants. However, the nature of the questions is not sensitive or invasive, which minimizes any potential harm or discomfort for the participants.

Studies involving observation:

Confirm whether participants will be asked for their informed consent to be observed.

Yes ☐ No ☒

Will you debrief participants at the end of their participation (i.e. give them a brief explanation of the study)?

Yes ☒ No ☐

Will participants be given information about the findings of your study? (This could be a brief summary of your findings in general)

Yes ☒ No ☐

Section 4: Data Storage and Security

Confirm that all personal data will be stored and processed in compliance with the Data Protection Act (1998)

Yes ☒ No ☐

Who will have access to the data and personal information?

- Only the primary researcher and supervisors involved in the study will have access to the data.

During the research:

Where will the data be stored?

- The data will be stored on a secure server with password protection.

Will mobile devices such as USB storage and laptops be used?

Yes ☒ No ☐

If **"YES"**, please provide further details:

- Mobile devices such as laptops may be used for data analysis. All devices will have secure, password-protected access. Data will not be stored permanently on these devices and will be removed after analysis.

After the research:

Where will the data be stored?

- The data will be stored on a secure server with password protection.

How long will the data and records be kept for and in what format?

- Data and records will be kept for five years in a digital format.

Will data be kept for use by other researchers?

Yes ☐ No ☒

If **“YES”**, please provide further details:

Section 5: Ethical Issues

Are there any particular features of your proposed work which may raise ethical concerns? If so, please outline how you will deal with these:

It is important that you demonstrate your awareness of potential risks that may arise as a result of your research. Please consider/address all issues that may apply. Ethical concerns may include, but are not limited to the following:

- Informed consent.
- Potentially vulnerable participants.
- Sensitive topics.
- Risks to participants and/or researchers.
- Confidentiality/anonymity.
- Disclosures/limits to confidentiality.
- Data storage and security, both during and after the research (including transfer, sharing, encryption, protection).
- Reporting.
- Dissemination and use of your findings.

Section 6: Declaration

I have read, understood and will abide by the institution’s Research and Ethics Policy:

Yes ☒ No ☐

I have discussed the ethical issues relating to my research with my Unit Tutor:

Yes ☒ No ☐

I confirm that to the best of my knowledge:

The above information is correct and that this is a full description of the ethics issues that may arise in the course of my research.

Name:	Ryan Wickramaratne
Date:	21/07/2023

Please submit your completed form to: ESOFT Learning Management System (ELMS)

List of figures

TABLE OF CONTENTS

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.

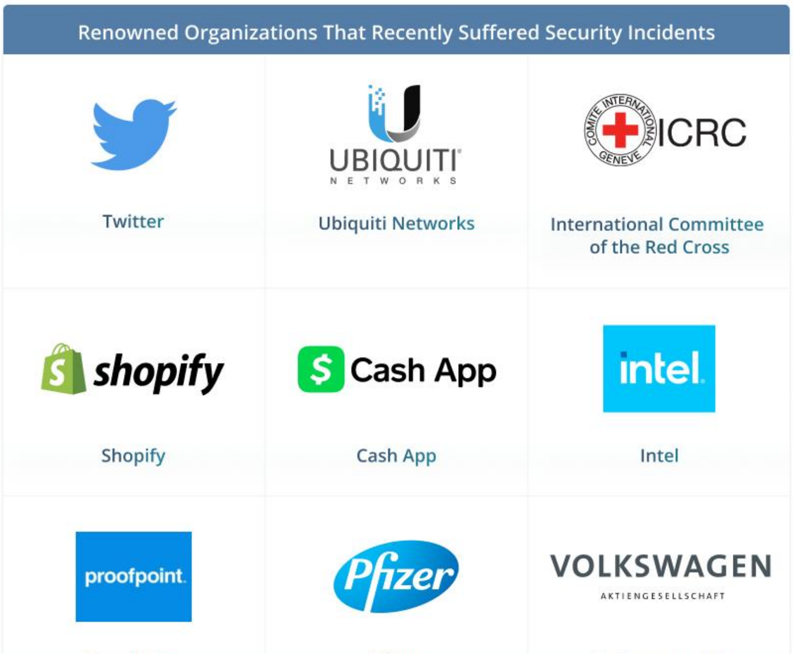

Renowned Organizations That Recently Suffered Security Incidents
Twitter
UBIQUITI NETWORKS
Ubiquiti Networks
ICRC
International Committee of the Red Cross
shopify
Shopify
Cash App
Cash App
intel
Intel
proofpoint
Pfizer
VOLKSWAGEN AKTIENGESELLSCHAFT

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.

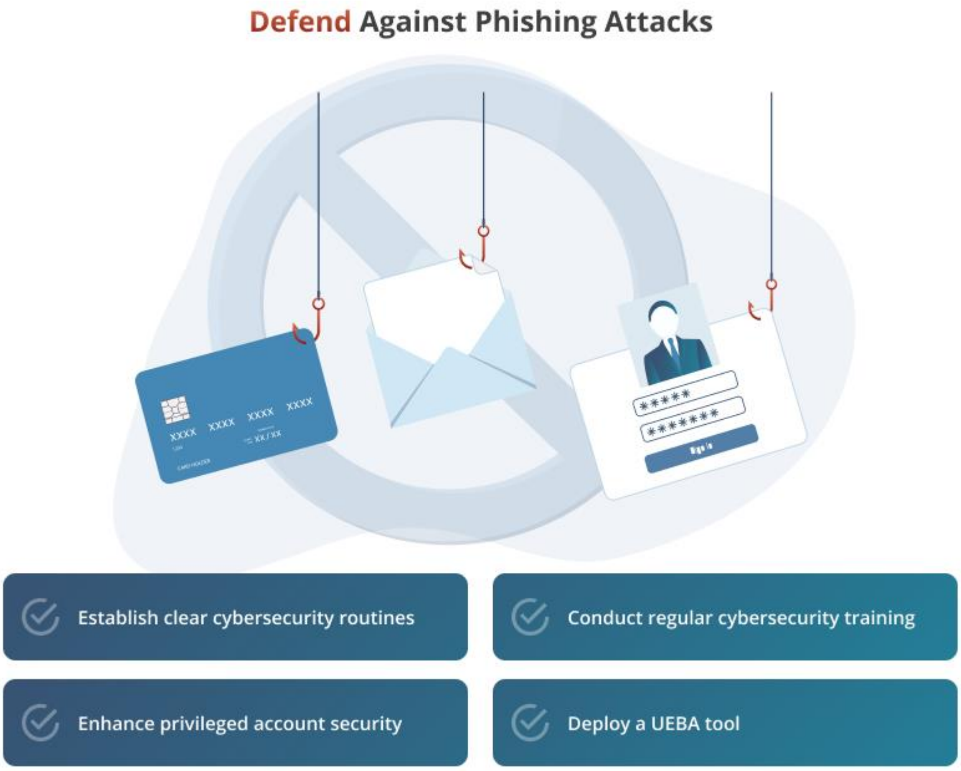

Defend Against Phishing Attacks
XXXX XXXX XXXX XXXX
XX / XX
CARD HOLDER
*****
****
Sign in
Establish clear cybersecurity routines
Conduct regular cybersecurity training
Enhance privileged account security
Deploy a UEBA tool

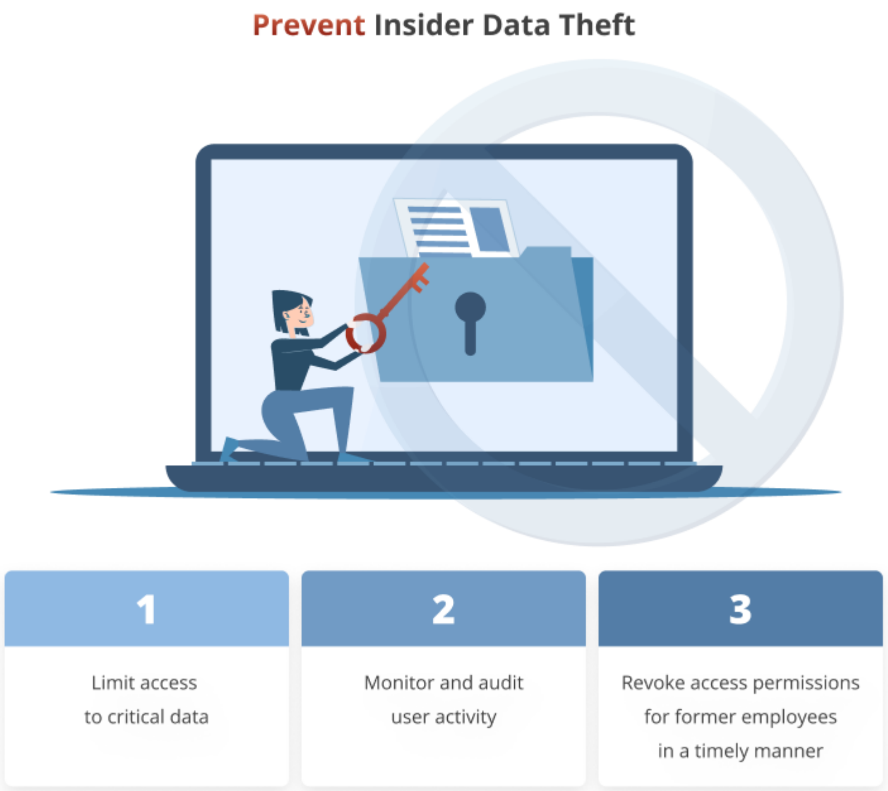
Figure 3 Ways to defend against phishing attacks

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

1 Limit access to critical data

2 Monitor and audit user activity

3 Revoke access permissions for former employees in a timely manner

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.

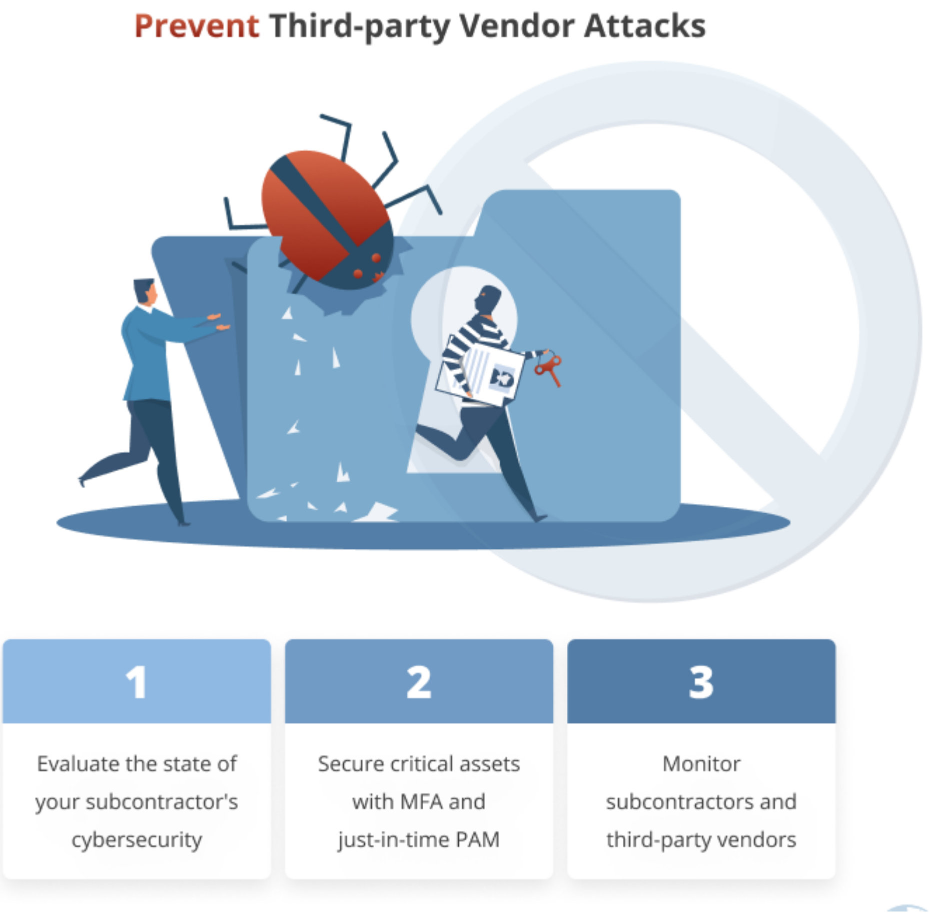

Prevent Third-party Vendor Attacks
1
Evaluate the state of your subcontractor's cybersecurity
2
Secure critical assets with MFA and just-in-time PAM
3
Monitor subcontractors and third-party vendors

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.

(EKRAN, 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.

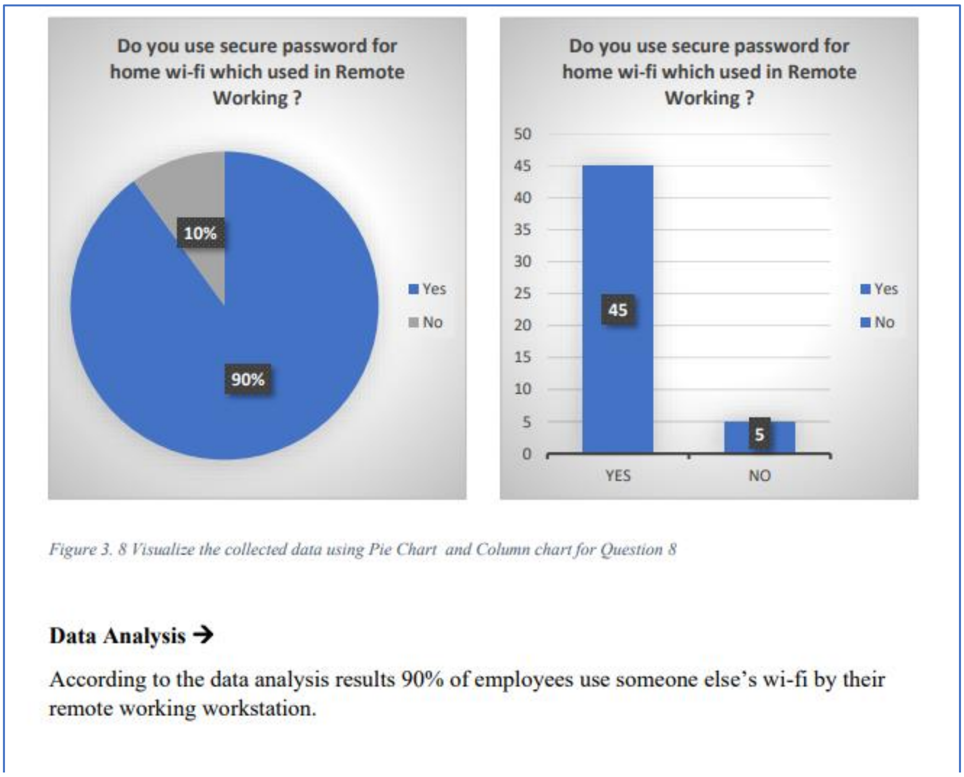


Figure 3. 8 Visualize the collected data using Pie Chart and Column chart for Question 8

Data Analysis →

According to the data analysis results 90% of employees use someone else's wi-fi by their remote working workstation.

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.

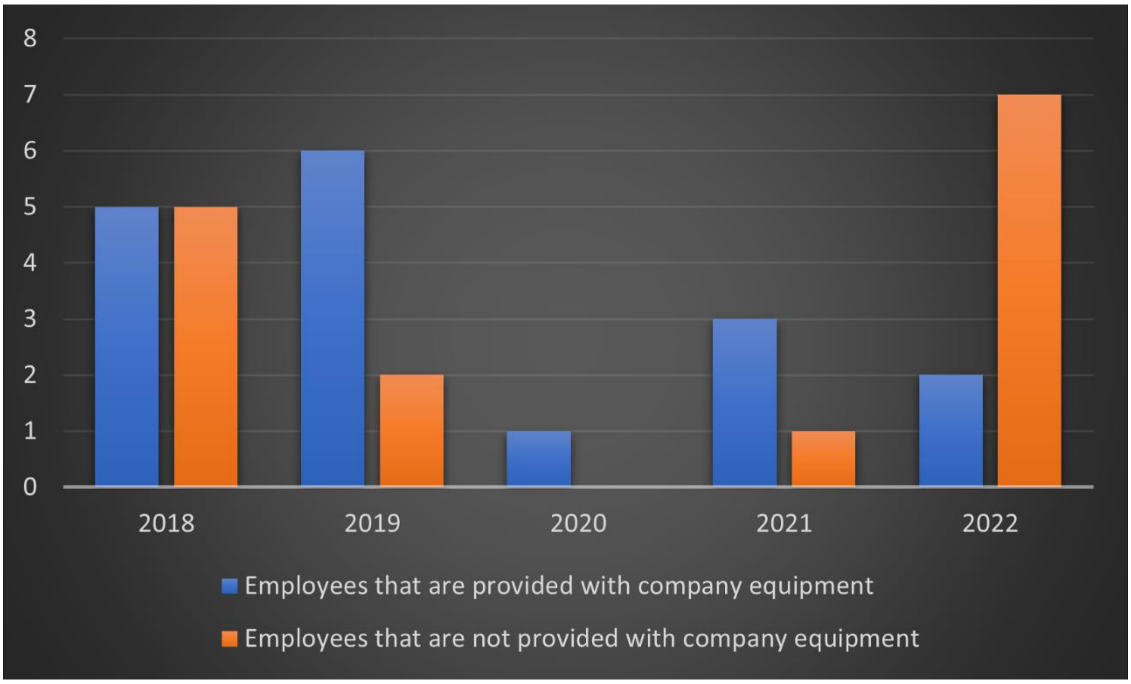


Figure 7 The number of employees recruited each year with or without remote working equipment by the company

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.

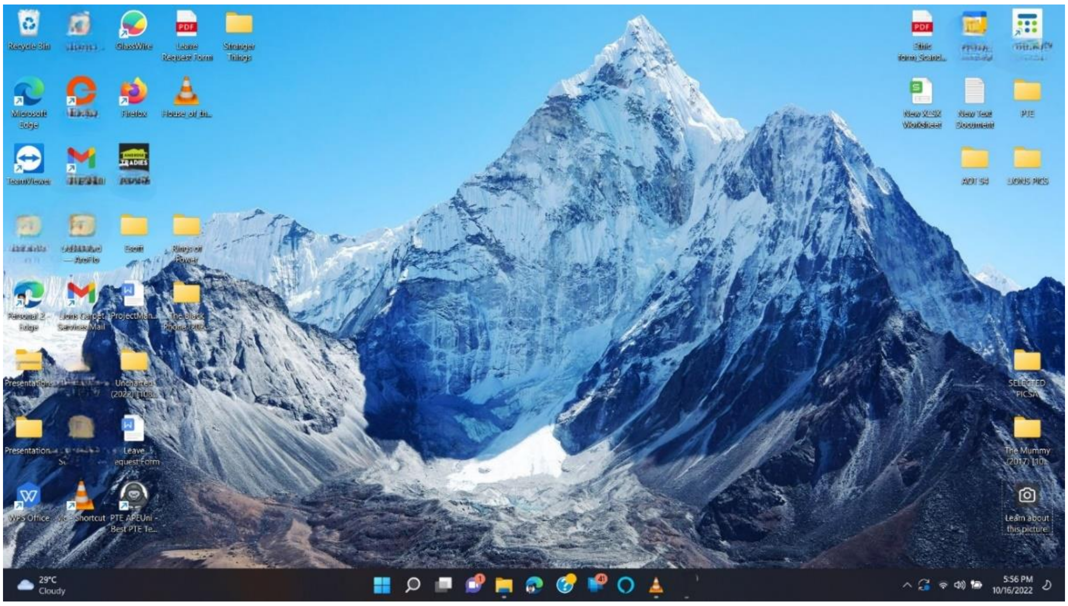


Figure 8 Past employee desktop screen shot with having company and personal data mixed up

The system analysist 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.

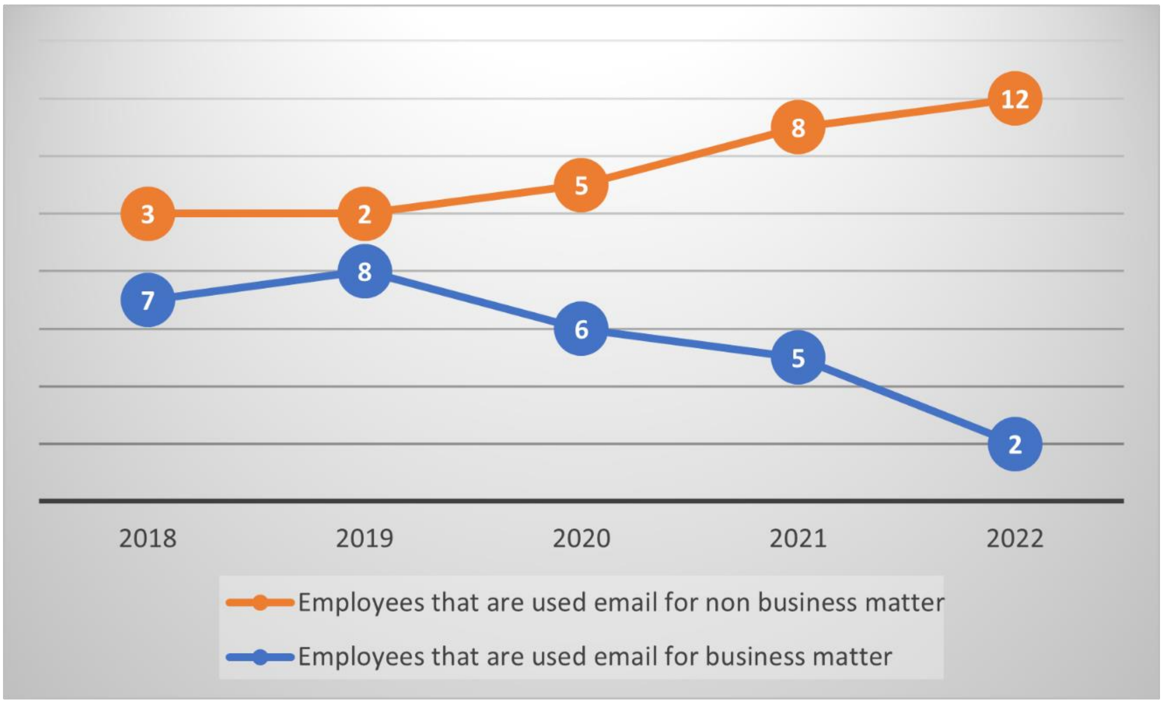


Figure 9 Number of employees used their corporate email for unauthorized web sites and not

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.

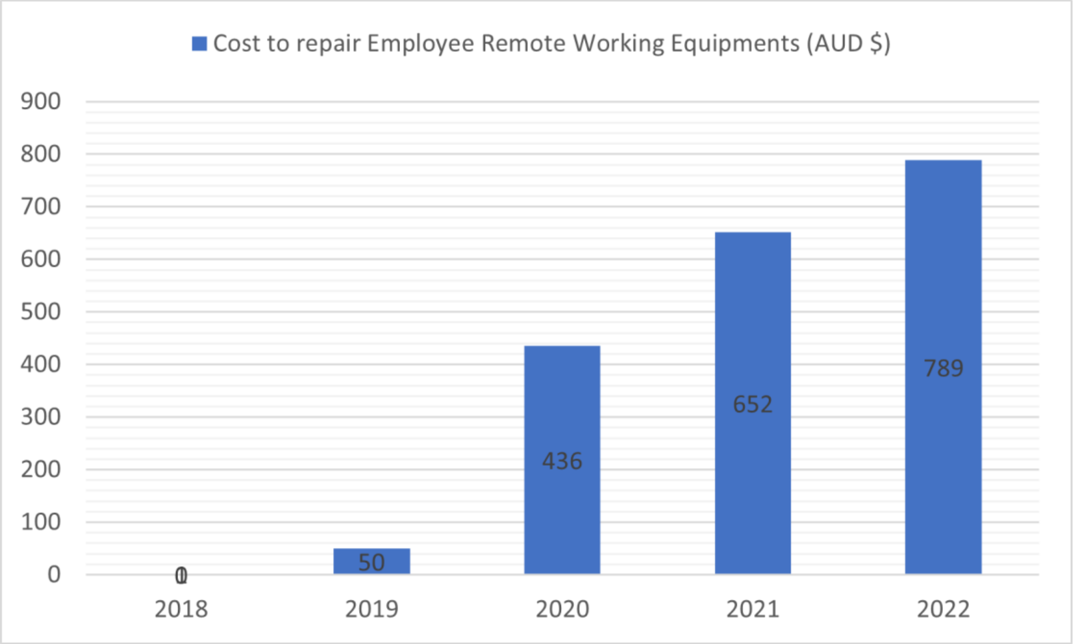


Figure 10 Cost sheet on equipment repairs and maintenance for remote workers

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

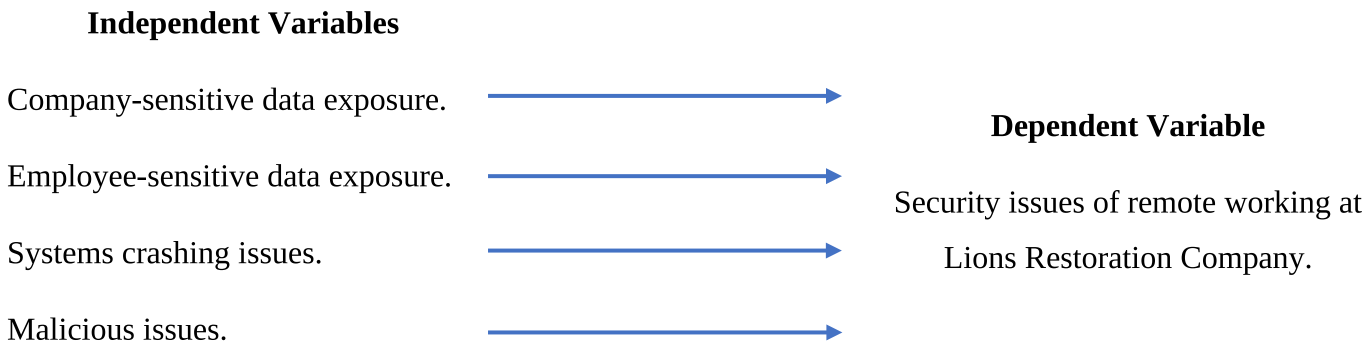
Research Question 1 : Is company sensitive data exposure caused by remote working at Lions Restoration Company?

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

Company-sensitive data exposure.

Employee-sensitive data exposure.

Systems crashing issues.

Malicious issues.

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

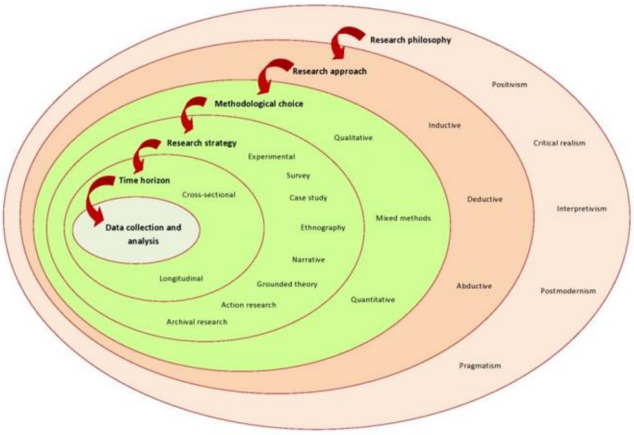


Figure 11 Research Onion

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 made up of six fundamental parts that work together to create a thorough research project. The first layer is research philosophy, which describes the researcher's viewpoint and method of conducting research. Research Methodology, the second layer, is based on the selected research philosophy. The third layer is the research strategy, which describes the overall strategy that will be used to accomplish the research goals. The fourth layer, Time Horizon, deals with how long the researcher plans to spend gathering data. Data Collection, the fifth layer, deals with the techniques used to gather data. Data Analysis, the last layer, deals with the analysis of the gathered data. Each of these elements should be taken into account while planning and carrying out a research study.

3.2 Research Philosophy - Positivism

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.

3.3 Research Approach - Deductive

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.

3.4 Research Choice – Mono Method Quantitative

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.

3.5 Research Strategy – Mono Method Questionnaire

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.

3.6 Time Horizon – Cross Sectional

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.

3.7 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 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.

References

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

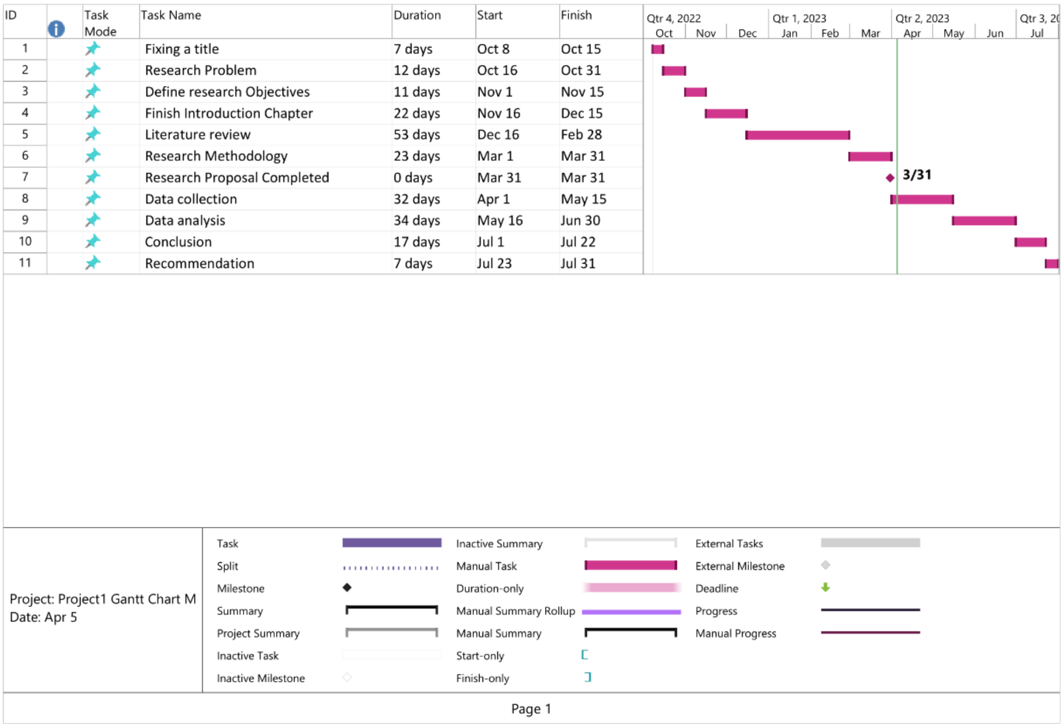
IBM Security. (2021). Cost of a Data Breach Report 2021. https://www.ibm.com/security/data-breach

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

Appendix – 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)



ID	ℹ	Task Mode	Task Name	Duration	Start	Finish
1		📌	Fixing a title	7 days	Oct 8	Oct 15
2		📌	Research Problem	12 days	Oct 16	Oct 31
3		📌	Define research Objectives	11 days	Nov 1	Nov 15
4		📌	Finish Introduction Chapter	22 days	Nov 16	Dec 15
5		📌	Literature review	53 days	Dec 16	Feb 28
6		📌	Research Methodology	23 days	Mar 1	Mar 31
7		📌	Research Proposal Completed	0 days	Mar 31	Mar 31
8		📌	Data collection	32 days	Apr 1	May 15
9		📌	Data analysis	34 days	May 16	Jun 30
10		📌	Conclusion	17 days	Jul 1	Jul 22
11		📌	Recommendation	7 days	Jul 23	Jul 31

Project: Project1 Gantt Chart M
Date: Apr 5

Page 1