Text

Description automatically generated with medium confidence

**School of Science and Technology**

**INVESTIGATION AND MITIGATION OF RANSOMWARE**

SUPERVISED BY (SUPERVISOR’S NAME)

“Project Report submitted in partial fulfillment of the requirements of Nottingham Trent University for the degree of MSc IT Security”.

YOUR NAME (STUDENT NUMBER)

AUGUST 2024

# **ABSTRACT**

This dissertation focuses on the ransomware detection and its prevention as a relatively new form of cyber threat that poses great risks to various organizations around the world. In this research, effective framework is developed that will improve the identification of ransomware threats and reduce the occurrence and the effects of the same. Based on a critical review of exiting literatures, the study establishes the advantages and the disadvantages of the existing detection techniques with respect to signature-based and behavior-based techniques. It puts forward the use of technologies like artificial intelligence and machine learning for better precision and flexibility. It also investigates understanding measures that can be taken to prevent such vulnerabilities which include, ensuring that software is up to date, adopting MFA, and user awareness programs. Further, it underlines the value of response planning, legal and compliance frameworks as well as sustained research and response improvement for the effective countermeasures against ransomware attacks. Thus, sharing some insights into ransomware mitigation measures in this dissertation, the author contributes into the general knowledge of ways organizations can protect themselves from ransomware attacks. Thus, the results point to such key tenets as multiple lines of defense, the role of people in cybersecurity, and the importance of the international approach to addressing ransomware threats. Regarding the future research avenue, suggestion for future studies include exploring new ransomware types, effects of the advanced technologies and the consequences of the ransom amounts, offering a pathway of research line for further advancement in this area of study. Beyond considering the existing threats and providing an understanding of ransomware and its prevention, this work contributes also to the development of further studies in the field of cybersecurity to protect data and other digital resources all over the world in the context of global interconnection.

# **ACKNOWLEDGEMENTS**

Firstly, I would like to extend my appreciation to my supervisor, for his assistance, encouragement and challenge that has enabled me to develop both intellectually and spiritually. I would also run my appreciation to friends and families who stood by me and mostly to my lovely wife for her support and understanding throughout the process. This they have been encouraging me and I would not have been able to accomplish this while they left me alone.

Thank you for the labour and inspiration in this period once more.

**TABLE OF CONTENTS**

[**ABSTRACT** 2](#_Toc175839085)

[**ACKNOWLEDGEMENTS** 3](#_Toc175839086)

[**CHAPTER ONE: INTRODUCTION** 6](#_Toc175839087)

[**1.1** **Background to the Study** 6](#_Toc175839088)

[**1.2** **Problem Statement** 8](#_Toc175839089)

[**1.3** **Aim and Objectives** 9](#_Toc175839090)

[**1.4** **Significance of the Study** 10](#_Toc175839091)

[**1.5** **PSEL Issues** 11](#_Toc175839092)

[**1.6** **Structure of Dissertation** 12](#_Toc175839093)

[**CHAPTER TWO: LITERATURE REVIEW** 14](#_Toc175839094)

[**2.1** **Introduction** 14](#_Toc175839095)

[**2.2** **Definition of Ransomware** 14](#_Toc175839096)

[**4.1** **Overview of Colonial Pipeline Ransomware Attack** 17](#_Toc175839097)

[**2.5.1**  **Classification by Target** 22](#_Toc175839098)

[**2.5.2**  **Classification by Infection Vectors** 25](#_Toc175839099)

[**2.6** **Ransomware infection path** 26](#_Toc175839100)

[**4.2** **Detecting ransomware** 28](#_Toc175839101)

[**3.1 Introduction** 33](#_Toc175839102)

[**3.2 Research Design** 34](#_Toc175839103)

[**3.3 Data Collection Methods** 34](#_Toc175839104)

[**3.4** **Inclusion and Exclusion Criteria** 36](#_Toc175839105)

[**3.5** **Data Analysis Techniques** 37](#_Toc175839106)

[**3.6** **Ethical Considerations** 38](#_Toc175839107)

[**CHAPTER FOUR: ANALYSIS AND FINDINGS** 40](#_Toc175839108)

[**4.1** **Introduction** 40](#_Toc175839109)

[**4.2** **Attack Methodology: A Review of the Colonial Pipeline Ransomware Attack** 41](#_Toc175839110)

[**4.3** **Evaluation of the effectiveness of current mitigation strategies against ransomware attacks** 45](#_Toc175839111)

[**4.4** **Identifying gaps and limitations in the existing detection and mitigation frameworks.** 49](#_Toc175839112)

[**4.5** **Mitigation Techniques in Ransomware Attacks: Colonia Pipeline** 53](#_Toc175839113)

[**4.6** **Proposed Detection and Mitigation Framework** 57](#_Toc175839114)

[**4.7** **Summary** 65](#_Toc175839115)

[**CHAPTER FIVE: SUMMARY CONCLUSION, RECOMMENDATION AND SUGGESTION FOR FURTHER STUDIES** 66](#_Toc175839116)

# **LIST OF TABLES**

[Table 1: Inclusion and Exclusion Criteria 37](#_Toc175840674)

[Table 2: Thematic analysis of the evaluation of the effectiveness of current mitigation strategies against ransomware attacks 48](#_Toc175840675)

[Table 3: Thematic analysis to identify gaps and limitations in existing detection and mitigation frameworks for insider threats 52](#_Toc175840676)

# **CHAPTER ONE: INTRODUCTION**

## **1.1** **Background to the Study**

Methods of cyber extortion have existed since the 1980s. The PC Cyborg Trojan was the earliest ransomware example, dating back to 1989 (Tailor, Patel 2017). PC Cyborg masked folders and encrypted the names of all files on the C drive after restarting the target machine 90 times, making the system inoperable. Ransomware attacks were largely carried out in the 1990s and early 2000s by amateur hackers looking to acquire a reputation via cyber pranks and destruction (Srinivasan 2017). Around 2005, modern ransomware arose and rapidly became a viable commercial tactic for attackers (Wilner et al. 2019). To get greater ransoms, targets switched from people to businesses and organizations (et al. 2019). Transportation, healthcare, financial sectors, and government were specifically targeted (Alshaikh et al. 2020).

Ransomware has emerged as one of the most severe computer threats, and the number of threats confronting corporations, public sectors, industries, and IoT devices has grown dramatically in recent years (Yaqoob et al., 2017; Faghihi & Zulkernine, 2021). Even though ransomware has been around for over 30 years, its first impacts were low, impacting only a small number of people, and the recovery procedure was straightforward (Salvi & Kerkar, 2017). However, as IoT has matured, ransomware assaults have grown dramatically, peaking around 2012 (Humayun et al., 2021). In 2019, at least 966 government, educational, and healthcare organizations were hit by ransomware attacks, costing the US economy an estimated $7.5 billion (Emsisoft Malware Lab, 2019). These attacks have sometimes endangered lives by interfering with emergency services or redirecting patients to other hospitals (Reilly, 2019). Ransomware attacks are estimated to inflict more than $200 billion in damage by 2021 (Humayun et al., 2021). As a result of widely accessible ransomware toolkits and ransomware-as-a-service (RaaS) that enable amateurs to launch ransomware assaults, the number of ransomware attacks has increased tremendously (Sharmeen et al. 2020).

Ransomware attacks may inflict considerable financial damage, lower productivity, interrupt routine business processes, and ruin people's or firms' reputations (Jain, Rani 2020). According to the findings of the global survey 'The State of Ransomware 2021' commissioned by Sophos, the average total cost to an organization to rectify the impacts of a ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid, etc.) was US$1.85 million, which is more than double the US$761,106 cost reported in 2020 (ran, 2021). These assaults may potentially result in irreversible data or file loss. Paying the ransom does not ensure the release of the locked machine or data (for Cyber Security, 2018). The cost of recovering from an assault double on average for organizations that pay the ransom (Ltd. 2020). Ransomware attacks are estimated to cost the globe $20 billion by the end of 2021, up from $325 million in 2015 (Alshaikh et al. 2020). Since the COVID-19 epidemic, these assaults have been extremely damaging, beginning with hospitals, vaccine research facilities, and contact tracking applications (Pranggono, Arabo 2021). All these figures indicate that we need to better understand the behaviour of ransomware and its variations to prevent and mitigate future attacks. Ransomware variations that avoid regular antivirus software and other detection measures continue to evolve because of their profitability. As a result, it is important to develop a new generation of effective countermeasures (Beaman et al. 2021).

Almost all firms have difficulty detecting ransomware (Thomas & Gallagher, 2018; Brewer, 2016). Attackers with access to storage devices encrypt system data and make systems inoperable (Brewer, 2016). Since its inception, ransomware attacks have grown in complexity and severity, with more recent versions encrypting user data employing a combination of symmetric and asymmetric encryption (Davies et al., 2020). Such attacks have major consequences, such as businesses ceasing operations, consumers losing access to services, and reputations being harmed (Thomas et al., 2019). Security experts and ransomware developers are always engaged in an "arms race" to safeguard their digital infrastructure from such attacks.

## **1.2** **Problem Statement**

Ransomware continues to pose as one of the most rampant threats in the field of cybersecurity and has led to massive losses in form of monetary and time losses to individuals, companies, and governments from all over the world. Traditional cybersecurity measures have not been effective enough against the evolving ransomware attacks thus the significance of new detection/countermeasures. According to CISA (2020), ransomware attacks have significantly rose with huge down time, data losses, and expensive recovery costs. These attacks that include the locking of important data by the hackers then asking for ransoms, disrupt critical infrastructure and services and will lead to major economic and social consequences.  
In the new generations of ransomware there are several features that make them work almost invisible; for instance, they use tricks like obfuscation and polymorphism, zero-day exploits, etc.

In this regard, attackers seek to use social engineering and phishing threats, which guarantee their threats are not detected using conventional antivirus software (Kharraz et al. , 2015). This increasing complexity demands fresh solutions for ransomware threats identification and prevention. However, there is still a significant risks and uncertainties about the legal and ethical implication of combating ransomware. Adding to the concern of having to pay the ransom in most cases against the set regulatory policies and ethical considerations is the concern of getting back to business as soon as possible. Lack of correlation of standard specific guidelines and due to complicated legal environment, it becomes very difficult to manage ransomware effectively (Martin et al. , 2018).

A review of the literature shows that there are several frameworks and methodologies suggested to counter ransomware threats. Currently, Kapoor et al. (2021) proposed the DAM model that collectively provides protection regarding ransomware detection, avoidance, and protection against its consequences. In the same year, Oz et al., (2022) pointed towards the importance of understanding different families of ransomware and their defense mechanisms needed to be developed. Kang & Gu, (2023) focused on the difference between Static and Dynamic Threat Detection techniques. However, there remains a significant gap in research that entails the full integration of the technical, legal, and ethical areas of ransomware mitigation, stressing the need for empirical investigations of the effectiveness of the present anti-ransomware mechanisms and approaches.

## **1.3** **Aim and Objectives**

The aim of this study is to establish a framework and a set of detection and defense techniques that can effectively protect against ransomware attacks; to fill research gaps that have not yet been addressed by previous scholarship and to offer specific recommendations to cybersecurity analysts and practitioners. The corresponding specific objectives in respect of the aim of this dissertation are as follows:

1. reviewing the literature on ransomware within the next three months to evaluate its comprehensiveness to study the recent ransomware attacks, patterns of its distribution and execution.
2. analyse and assess current approaches and methods for determining the presence of ransomware in today’s computing scenarios.
3. analyse the current situation of ransomware attack mitigation and indicate areas of strength and weakness.
4. proposed at least three other possible approaches for dealing with ransomware, considering recognized deficiencies in the current measures.
5. suggest a detection and mitigation of ransomware attack since current detection and mitigation methods are inefficient.

## **1.4 Significance of the Study**

The significance of this study is in the potential to advance knowledge and practice of cybersecurity improving the ability to counter ransomware threats. The research is relevant and important, especially with the increasing rate of ransomware attacks to the different areas of the world. First and foremost, this research proposal seeks to offer a general evaluation of the state of ransomware currently in the market. The research present an integrated approach to ransomware trends, delivery methods, and the general workflow of ransomware attacks by analysing the data from previous studies systematically. This overall comprehension is significantly important in the formulation of strategies and trends that would be effective on ransomware.

Secondly, methodological contribution of the study is relevant in practical terms for the assessment of cybersecurity. The insights derived from this research regarding efficacy of various anti-ransomware solutions and measures will be useful for cybersecurity specialist and corporations. The conclusions can serve as a useful guideline for constructing and deploying better defence strategies, which will improve the organisation’s preparedness against ransomware attacks. Also, the research focuses on the lack of empirical data as to the role of ransomware in risk management. Through the precise experiments and carrying out the comparison of the efficiency of different kinds of detection tools, the study will advance the knowledge of the best ransomware protection measures. It also makes the recommendations more realistic according to empirical observations rather than pure theory which narrows the gap of implementation of new knowledge.

Also, the study highlights ethical and legal concerns that surround the management of ransomware incidents. Through unfolding these dimensions, it is intended to offer a more broad-shouldered view of the state of art that would involve the ethical and legal pros and cons of varied measures of the mitigation ploy as well. It is necessary to design complete strategies for counteracting ransomware and creating effective and long-term solutions. Lastly, applicability of this study can be seen in terms of its contribution in presidential policy and practice. The insights gained from this research can inform policymakers, helping to shape regulations and guidelines that support effective ransomware mitigation. By contributing to a safer and more secure digital environment, this study addresses a pressing need in the field of cybersecurity.

## **1.5 PSEL Issues**

Ransomware is one of the most common and dangerous types of cyberthreats poses multiple challenges for professionals, societies, ethics and laws to fulfil to protect digital assets.

**Professional issues**: concerns that focus on the effectiveness and integrity of cybersecurity and proper adherence to several methodologies, which are rather important for right identification and countermeasures. Scientists must adhere to laid down guidelines to manage data honesty and security, impartiality that eliminates prejudice that would jeopardize research credibility (Hudson, 2020; Ghazinoory et al. , 2014). Attention is paid to licensing and concern with privacy, as the issue of ethical handling of the information is critical (Williams, 2018).

**Social Issues**: the social consequences of ransomware research are vast and significant especially with regards to the preservation of the rights of individuals and espousing the providence of social norms. Researchers must pay attention to how their findings comport with the communal standards, address how the results might harm society and diligence on justice to minorities in their research (Elliott et al., 2018 ; Hudson, 2020).

**Ethical Issue**: When involving human participants, it is critical to recognize and apply what ethical consideration especially the key principle of conducting research namely, autonomy of the participants, beneficence, and justice while engaging human participants. For ethicality, the acknowledgement of decisions or involvement with research and the fair share of benefits derived from such research should be observed (Beauchamp & Childress, 2019; Resnik, 2015).

**Legal Issues**: This complicates the pattern further, as strict adherence to intellectual property laws, data protection regulations such as the GDPR, and institutional ethical guidelines is crucial (Regulation (EU) 2016/679; U.S. Department of Health & Human Services). Researchers must obtain ethical approvals and ensure compliance with relevant legal frameworks to avoid potential legal consequences (Hudson, 2020)..

## **1.6 Structure of Dissertation**

This dissertation is broken down into 5 chapters. This chapter which is the first chapter is the introduction of the dissertation which provides the background to the dissertation.

Chapter 2 provides a comprehensive overview of existing literature relevant to ransomware investigation and mitigation. It critically examines various perspectives and methodologies presented in previous research and identifies key themes and gaps in the literature. The review focuses on understanding how ransomware is delivered, the forensic procedures used in investigations, and the strategies employed for mitigation. By synthesizing and analysing these studies, this chapter helps to contextualize the study within the broader field of cybersecurity.

Chapter 3 provides the research design and methodology of this dissertation. Since the proposed investigation is of a quantitative type, this chapter provides information about the identification and selection of secondary data with the help of an extensive literature review, as well as the reason for choosing thematic analysis as the method of data analysis. It also highlights techniques and methods used in the study when selecting participants; inclusion and exclusion criteria used to define the participants that were targeted. Moreover, the chapter explores the ethical concerns relevant to the research and eradicates any violation of ethical code of practice a research study may be prone to.

This chapter 4 summarises the findings of the thematic analysis that was conducted regarding the selected literature. In discussing the findings of the study, the chapter is structured in reference to the themes developed during the analysis of the research questions. The discussion finalises these findings by explaining how they relate the current literature and how the research contributes towards the understanding of ransomware investigation and prevention. It also looks at the meaning and significance of the research with regards to the future advancement of theory and practice to be of value in developing other research projects in the field of cybersecurity.  
  
Chapter 5 of the dissertation presents the major conclusions of the study conducted in the research. This relates to the research objectives and questions to how they have been addressed in the study. Furthermore, this chapter provides the directions for further research and proof of concept templates for ransomware investigation and prevention. It also describes the research limitations, which point to the directions in which the research information developed in this dissertation could be expanded. In more concrete terms, this chapter provides a final review of the research done and the implications that it has on the science of cybersecurity.

# **CHAPTER TWO: LITERATURE REVIEW**

## **2.1** **Introduction**

Ransomware attack have become a significant cybersecurity threat that present serious risk to its victims, including individuals, enterprises, and states (Kharraz et al. , 2015). They are malicious software that encrypt the files or restrict the access to the computer systems and then demand money from the victims. Hence, to comprehend ransomware in its detail, a full understanding of the basic operating, ways of infiltration and possible protection measures is required. Previous studies have paid attention to the detection of ransomware through network traffic analysis, static and dynamic analysis of the malware, and the ransom notes and Bitcoins transactions among other (Gupta et al. , 2017; Abrams et al. , 2020).

Ransomware identification is very important to minimize loss of data as well as high financial losses. The approaches that can be effectively employed include the use of signature-based scanning where the apparatus look for recognizable patterns which are associated with threats (Scaife et al., 2016); the use of behaviour-based scanning, where the apparatus focuses on activities that resemble ransomware activities (Pawar et al., 2020); and machine learning techniques such as detection of anomalies and classification (Buczak & Guven, 2016).

Different work cover ransomware in various angles, due to the definitions given which involve extortion, encryption, restrict access, data theft, and exposure (Kharraz et al. , 2018; Christin, 2017). Such differences explain why dealing with ransomware threats is complex.

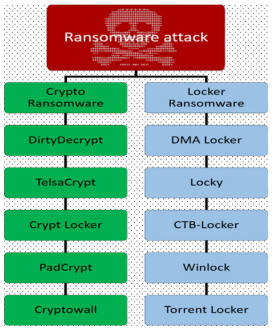
## **2.2** **Definition of Ransomware**

Ransomware is a type of malicious software which encrypts information belonging to a victim and demands payment for its decoding. This kind of online blackmailing has grown popular and more sophisticated as pointed with various researchers. As stated by Yaqoob et al. (2017), these cybercrimes involve payment in bitcoins, and this has been confirmed by Sophos (2019) to be on the rise and posing a great threat to internet users. Ransomware is defined as a scaled-up sub-set of malwares, which is a generalized classification of viruses, worms, rootkits, botnets and Trojan horses (Grégio et al., 2015).Ransomware specifically targets both individuals and organisations globally, with its primary function being to block access to an infected system until a ransom is paid (US-CERT, 2016). The more dangerous variant, crypto ransomware, employs sophisticated encryption algorithms to lock users out of their data, often appending a new file extension to encrypted files (Dubey, 2016). Victims are typically informed of the attack through a notification that provides instructions on how to pay the ransom and retrieve their data (Trend Micro, n.d.). Although several types of ransomwares exist, this paper will focus on crypto-ransomware, which, as Steinberg (2018) notes, is the most prevalent and destructive form.

The role of encryption is central to most definitions of ransomware. Ritter et al. (2017) describe ransomware as software that encrypts data and demands a ransom for decryption, with the primary objective being extortion through encryption. According to Christin (2017), the definition must be broader and encompass file encryption alongside the prevention of access to the entire computer system while pointing at the psychological pressure on the victim to pay the ransom. These two paradigms demonstrate duality of ransomware as threat to encryption of data, and as a tool of forceful denial of access. Leveraging social engineering is critical to ransomware attacks as described by Pawar et al. (2020) where they capture various mainstream heinous stunts used to compel users to initiate the payload. This aspect greatly emphasizes on the fact that ransomware is manipulative and takes advantage of people’s weakness. Kharraz et al. (2018) also note that there is yet again a problem of defining ransomware in relation to other types of malwares that may have similar behavior but serve a different purpose, for instance, wipers or spyware. According to these researchers, one parameter has remained particularly important when defining ransomware and this is the intent of the attackers to cash-in a ransom from the user of the targeted device.

Reaves et al. (2016) propose a new meaning of the ransomware threat that should take into consideration its developments, including the aspect of data encryption or theft and disclosure. This broader definition takes into considerations the newer forms of ransomware that are more dangerous than traditional ransomware in that they include features such as data leakage. Additional information about the variations in ransomware definitions and how they could complicate the situation and the communication process are given by Gröndahl et al. (2020). This underscores the need to come up with a common definition and understanding of ransomware as well as its classification to ensure that any line of defense against it is well coordinated. Other researchers, such as Morato et al. (2018), distinguish the behaviour of the various ransomware types, thus distinguishing between the lock-screen ransomware, which only prevents the user from accessing the computer, and encryption ransomware that does not let the user access the files. Other ransomware types are called wipers because they destroy the files and even if the ransom is paid the data cannot be recovered (O’Brien, 2017). The advancement from traditional ransomware to the new generation ransomware such as Ransomware-as-a-Service (RaaS), advanced by Petrasko (2017), has added the complexity with Cerber and Atom for example allowing individuals to carry out the attacks without prior knowledge. This has probably led to the emergence of more frequent ransomware attacks as noted by Thomas et al (2019).

Figure 1: Taxonomy of Ransomware attack



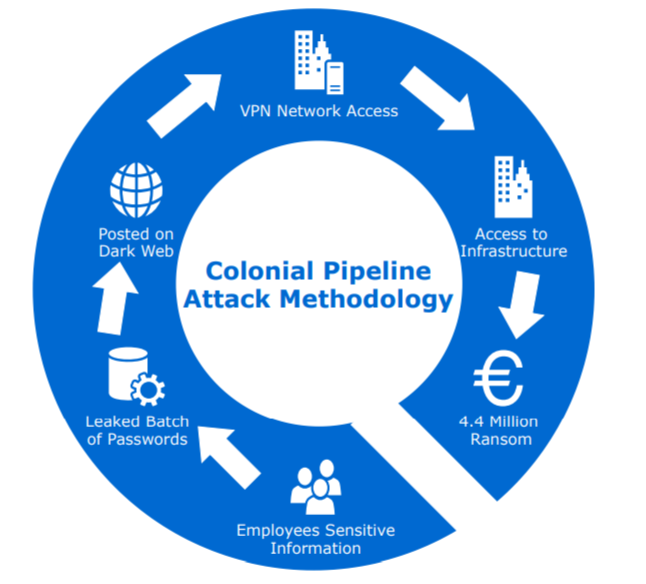
**Source**: Humayun et al. (2021)

Over the last several years, ransomware has become more dangerous. According to the Federal Bureau of Investigation (FBI), in 2015, there was a rise in ransomware attacks on organisations that law enforcement saw (FBI, 2016). According to Check Point, in the second half of 2016, ransomware assaults accounted for 10.5% of all malware attacks globally (Check Point, 2017a, 2017b). Research indicates that ransomware increases businesses' risk (Schulze, 2017; O'Brien, 2017). Due to a lack of backups and ransomware detection technologies, an organisation may sometimes be left with no choice but to pay the ransom (Palmer, 2017).

## **4.3 Overview of Colonial Pipeline Ransomware Attack**

In April 2021, Colonial Pipeline Co., the largest oil pipeline company in the United States, fell victim to a significant ransomware attack orchestrated by the hacking group DarkSide. The attack, which occurred on April 29, 2021, exploited vulnerabilities within the company's network, resulting in severe disruptions to the nation's fuel supply and prompting discussions on the cybersecurity of critical infrastructure. The Colonial Pipeline System is responsible for transporting over 2.7 million barrels of fuel daily, making it a vital asset for the United States, particularly for the Eastern states, where the impact of the attack was most keenly felt (Medlock III, 2021). The attackers infiltrated Colonial Pipeline's network through an old, inactive account linked to a virtual private network (VPN) as can be seen in Fig. 2. This account did not have multi-factor authentication (MFA) enabled, allowing the hackers to gain unrestricted access to the entire network using only the compromised credentials (Turton and Mehrotra, 2021). The exact method by which the hackers obtained the account password remains unclear. Possibilities include human blackmail, the reuse of an old password, or even a successful password guess, but the lack of MFA was a critical failure that facilitated the breach (Beerman et al., 2023). Once inside, the attackers were able to deploy ransomware, encrypting crucial data and demanding a ransom payment to restore access.

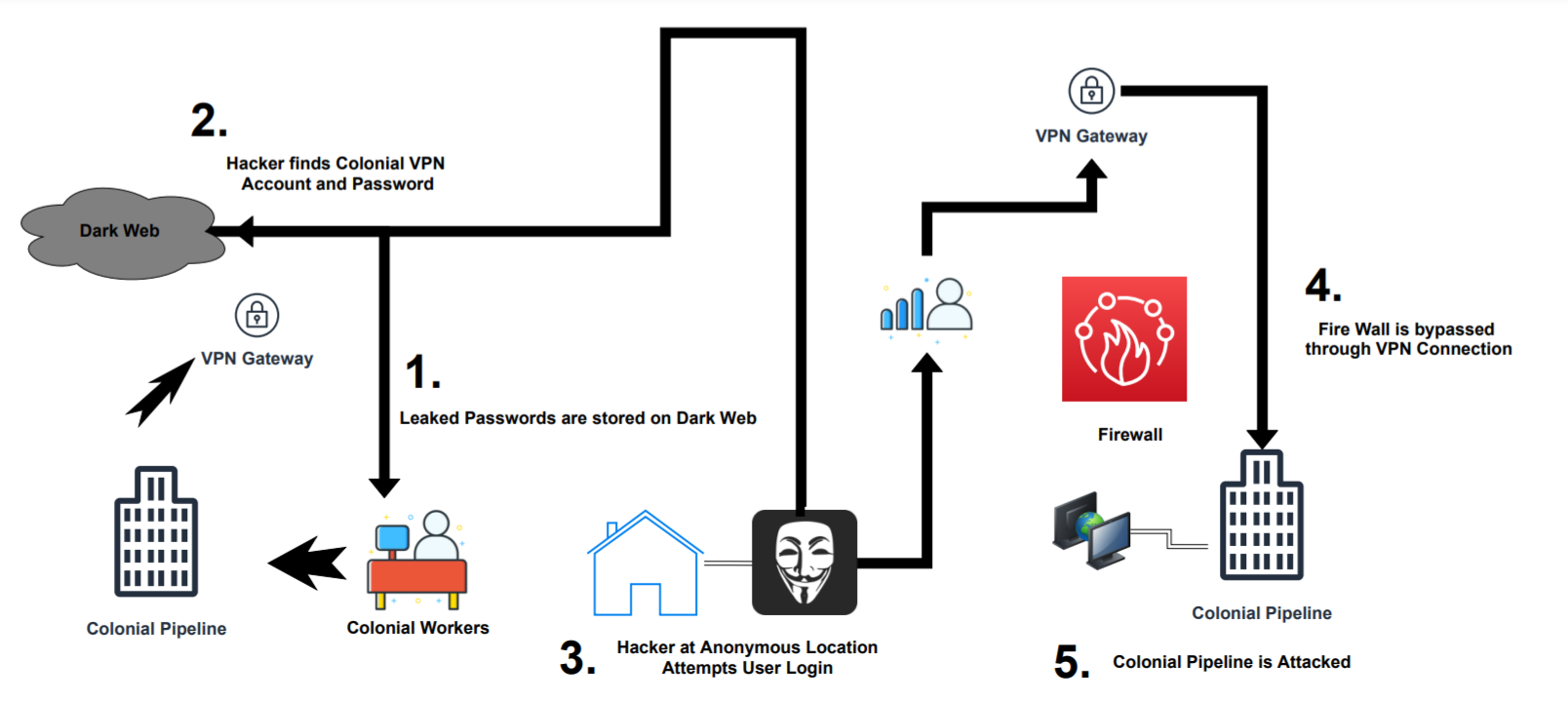
Figure 2: Taxonomy of Ransomware attack



Colonial Pipeline Co received the first ransom demand on the 7 of May 2021, which was about a week after the cyber-attack. $4.4 million in cryptocurrency. The latter demanded something which an employee received, and immediately informed his superiors about it. They have decided to pay the ransom which became one of the most discussed topics by the cybersecurity experts. Nevertheless, the pipeline was closed for a few days to identify the type of attack and how it was executed and prevent a reoccurrence (Beerman et al. , 2023). The attack highlighted significant weaknesses in the cybersecurity measures of critical infrastructure. Despite the rapid response, the shutdown of the Colonial Pipeline caused widespread fuel shortages along the East Coast, leading to panic buying and long queues at petrol stations. The disruption in fuel supply also showed how critical the Colonial Pipeline is to the United States or grasped how the lack of adequate cybersecurity endangers other fundamental services (Stephens, 2021).

A further investigation into the attack operation showed that the account that the attackers used to penetrate the VPN lacked MFA implemented, a severe mistake that the attackers exploited to enter the organization’s network. This breach led to the realization there is need to put in appropriate measures on cyber security especially in systems that are considered as critical infrastructure. The lack of MFA coupled with presence of a dormant, but active account linked to a critical system leaves a lot of doors open and hence the need eternal and effective security measures (Beermann et al. , 2023). As a result of the attack, Colonial Pipeline has made several upgrades in the security systems which consist of alarms inside the system. These alarms are intended to sound when any unauthorised access takes place in the future to stop hackers from roaming freely in the network of the company. Although this measure can be categorised under reactive security it is a step in the right direction towards enhancing the security of the pipeline operation. Figure 3 shows the flow of the Colonial Pipeline and the signs of the breach of security measures.

Figure 3: Process of Access to Colonial Pipeline Infrastructure



Moreover, the attack led to further discussion on how government has an obligation to protect the infrastructure of the country. The Colonial Pipeline which is under the “Critical Infrastructure vulnerable to attack” showed how chaos emanating from the involvement of such an asset could lead to severe outcomes including economic losses, and threats to national security. Trends have emerged upon the governments to be much more involved in cybersecurity especially through organizations such as the Cybersecurity and Infrastructure Security Agency (CISA) which is seeking to expand its mandate to protect crucial infrastructure. These proposals include increasing the team aspect of CISA’s approach and the formation of a Cyber Safety Review Board to write and look at lessons learned from cybersecurity events. (Smith and Monken, 2021).

The extension of ransomware to Colonial Pipeline attacked is a clear indication of the level of insecurity that continues to pervade the core civil infrastructural systems and structures all over the world. This brings out the fact that the implications are very serious as seen by the fuel scarcity and the general economic upheaval that was witnessed after the attack. It is now important that the experience that we have encountered must guide the strategies of preventing social structures that are crucial for the functioning of a state to be infiltrated with the same intensity by such a malicious group. Having a strong and up to date security for the critical infrastructure systems and MFA and reviewing the access protocols for critical systems are primary ways to reduce the other ransomware attacks (Voas et al. , 2021).The importance of securing critical infrastructure cannot be overstated, especially as the digital and physical realms continue to converge. The Colonial Pipeline attack has shown that the consequences of neglecting cybersecurity in such vital systems can be severe, affecting not only the operations of the targeted company but also the wider economy and national security. As the world becomes increasingly reliant on digital infrastructure, the need for robust and proactive cybersecurity measures will only grow more critical. Future incidents must be prevented by learning from past mistakes and implementing the necessary changes to protect against the ever-evolving threat pattern (Parfomak and Jaikaran, 2021).

**2.4 Taxonomy of Ransomware**

Ransomware is classed in many ways. As shown in Figure 3, we categorise ransomware based on its target and infection technique in this research. In this part, we first present a summary of each categorization category before classifying the most significant ransomware families using our technique.

## **2.4.1 Classification by Target**

Ransomware may be categorised according to its objectives into two orthogonal categories: target victim and target platform.

**Ransomware Victims**: Ransomware may target a wide range of victims. Analysing the characteristics of ransomware victims might give useful information for developing realistic defense methods. End-users and organisations are the two types of ransomware victims.

**End-users**: The main targets of the earliest ransomware families were end-users. Ransomware is particularly successful against end users because to a lack of security knowledge and technical help (Kevin Savage et al. 2015). Cryptographic ransomware may encrypt people's data that are kept on personal devices (e.g., PCs, laptops, cellphones, and so on). In the meantime, locker variations may lock end-user devices and block access until a ransom is paid. Unsurprisingly, the quantity requested by end-users is substantially smaller than the amount demanded by organisational objectives (Kevin Savage et al. 2015). Furthermore, a single ransomware infection may infect thousands of end-user computers, making it lucrative (Atapour-Abarghouei et al. 2019).

**Organisation**: Initially, organisations were not the primary targets of ransomware. However, as ransomware developed over time, many other sorts of organisations, including governments, hospitals, businesses, and schools, were routinely attacked. In these assaults, hackers pre-select their targets and aim to create maximum disruption in the expectation of receiving a large ransom payment (Jercich 2020). Locker ransomware may lock computers utilised in the target, potentially halting the whole operation (WIRED 2018). Similarly, cryptographic ransomware may encrypt important data stored in an organization's system and render it unavailable until a large ransom is paid. Cybercriminals may also threaten to make public their target's info.

**Ransomware Target Platforms**: Another important consideration in understanding ransomware behaviour is the target platform. Ransomware attacks a wide range of platforms. It is usually tailored to a single platform and operating system since it often makes use of system-specific libraries/functions (i.e., system calls) to carry out its malicious acts (Kevin Savage et al. 2015). In this research, we will use the words platform and operating system interchangeably, and we will categorise ransomware target platforms into three groups: PCs/workstations, mobile devices, and IoT/CPS devices are all examples of IoT/CPS devices.

**PCs/workstations**: PCs and workstations are the most typical targets for ransomware. Because of their ubiquity among consumers, the bulk of ransomware attacks PCs and workstations running Windows. Furthermore, several ransomware families, such as KeRanger for macOS and LinuxEncoder for GNU/Linux platforms, target different operating systems. Screen locker ransomware attacks may be mitigated by reinstalling the operating system. However, because of the use of modern encryption methods, it is almost hard to decode and retrieve data from cryptographic ransomware (Tang et al. 2020; Taylor 2023). As a result, cryptographic ransomware families are the most common threats to PCs/workstations.

**Mobile Devices**: Because of their rising prominence in society, mobile devices such as smartphones are good targets for ransomware. In terms of mobile devices, ransomware targets the Android and iOS platforms, which share the largest worldwide mobile OS market. Apple has a tightly regulated environment in which apps are extensively reviewed before being made available to users. This is most likely why iOS users have not been impacted by malware. There have only been incidents of phony ransomware for iOS devices (BBC 2017b). On the contrary, ransomware poses a danger to Android consumers owing to the open ecosystem of the Android platform. The first locker ransomware for mobile devices, Android Defender, appeared in 2013, targeting Android platforms, and the first cryptographic ransomware, Simplocker, appeared the following year (Lipovsk et al. 2015). Although cryptographic ransomware is more dangerous than locker variations on PCs/workstations, the converse is true for mobile ransomware. The fundamental rationale is that the impact of locker ransomware on PCs/workstations can be prevented most of the time by removing the hard drive, however, the same method is difficult for mobile devices (Snow 2016).

**IoT/CPS Devices**: At present, IoT and CPS devices are not the primary targets of ransomware outbreaks. However, such devices are becoming more common in a variety of deployment areas, including but not limited to smart homes, smart health, smart buildings, smart transportation, smart cities, smart manufacturing, and so on (Rondon et al. 2022). Indeed, Industrial IoT and CPS devices (e.g., PLCs, RTUs, RIOs, and so on) have already been powering industrial control systems in smart grids, water and gas pipelines, and nuclear and chemical facilities. Although ransomware for such systems is not widely used now, attackers may target such settings more often in the future (Dickson 2016).

## **2.4.2 Classification by Infection Vectors**

To infect their targets, ransomware writers utilise the same infection mechanisms as ordinary malware. Malicious e-mails, SMS or instant messaging (IMs), malicious programmes, drive-by-download, and vulnerabilities are the five types of ransomware infection tactics.

**Malicious e-mails** are the most typical ransomware infection vectors. Attackers send spam e-mails to victims with ransomware attachments (Sevtsov. 2017). Botnets may be used to spread such spam campaigns (Kurt et al. 2020). Ransomware may arrive with an attached malicious file, or the e-mail may include a malicious link that, when clicked, may install ransomware (drive-by download).

**SMS Messages or IMs:** SMS messages or instant messages are regularly utilised for mobile ransomware. In such cases, attackers send SMS messages or instant messaging to victims, instructing them to visit a rogue website and download ransomware onto their devices. Malicious Applications are employed by ransomware attackers who create and distribute mobile applications containing malware disguised as benign applications (Lipovsk et al. 2015).

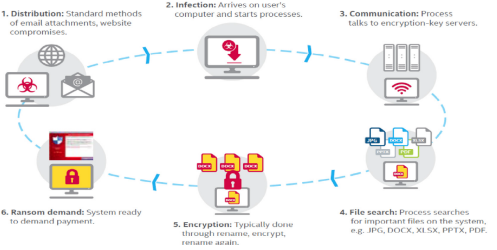
**Drive-by download:** Drive-by download occurs when a person visits an infected website or clicks on malicious advertising (i.e., malvertisement), and the malware is downloaded and installed without the user's awareness (Reuters Staff 2017).

**Vulnerabilities**: flaws in the victim platform, such as weaknesses in operating systems, browsers, or software, may be utilised as infection vectors by ransomware developers (BBC 2017a). Attackers may utilise exploit kits, or aid apps, to exploit known or zero-day vulnerabilities in target systems. Malvertisement and malicious links may be used by attackers to lead users to such kits.

## **2.6** **Ransomware infection path**

Wang and Wang (2015) claim that while exploiting a system's vulnerabilities, ransomware uses the same strategy as conventional malware. For instance, hacked websites or email attachments are used as attack vectors to infect a victim's machine. Many different organisations have put forth models that try to explain how ransomware behaves. According to several of them (Al-rimy, Maarof, and Shaid 2018), a ransomware assault may be classified into six different stages. The model shown in Figure 3 by McAfee (McAfee Labs 2016) is an illustration of such a concept.

Figure 4: McAfee 6 Phase Ransomware Model



(McAfee Labs, 2016)

**Distribution:** This stage involves delivering the malicious code to the victim's machine and packaging the ransomware. To make the distribution easier, a variety of exploitation tactics are used, including drive-by downloads, phishing assaults, spam mail campaigns, social engineering, and penetration (Davies, Macfarlane, and Buchanan 2020).

**Infection:** This stage focuses on how the ransomware operates and behaves at first. The malware investigates the operating environment at this phase and gathers data on the victim's device, including the platform type, OS version, and installed programmes (Prakash, Nafis, and Biswas 2017).

**Communication**: The ransomware pulls the encryption keys from the command and control (C&C) server at this stage. In order to provide the execution modules and encryption keys needed at a later stage of the infection, the attacker controls this remote computer. Not every ransomware performs this function since some variants already include the keys in their payload (Sgandurra et al. 2016). During this stage, some ransomware will attempt to switch to other computers on the network (Sophos, 2019).

**File Search**: The ransomware now begins searching for specific resources, such user files, resources, and accessibility features. Typically, file extensions are used to select files (Sultan et al., 2018).

**Encryption:** Depending on the family type, different ransomware hijacks and encrypts the targeted resources, with some (such as Petya) discarding the encryption key and others (such as Wannacry, NotPetya) communicating it back to the attacker through C&C server or ransom message. Hybrid key crypto ransomware (HCR), which uses a variety of encryption algorithms to improve speed, makes up the majority of contemporary ransomware. During this stage, files may be moved, renamed, or corrupted, and the MBR may also be encrypted. If ransomware executes secretly, a computer reboot could happen, which might be the first time a user notices the existence of ransomware (Davies, Macfarlane, and Buchanan 2020).

**Ransom demand:** After the encryption process is finished, the victim sees a message with payment instructions that demands a ransom. Although paying the ransom increases the likelihood of data recovery, it does not ensure that a decryption key will be sent (Richardson and North 2017).

## **2.7 Detecting ransomware**

This analysis seeks to critically review and assess the efficacy of existing ransomware detection techniques, ranging from traditional signature-based methods to more sophisticated machine learning, network-based, and hybrid approaches. By evaluating these techniques within the context of contemporary cybersecurity challenges, this analysis aims to highlight the strengths, limitations, and potential areas for improvement in ransomware detection strategies.

**1. Traditional Detection Techniques**

The traditional and primitive mitigation methods involve the regular methods of detection, which include signature and heuristic methods. Signature-based detection as pointed out by Bradley (2016) and Furnell & Emm (2017) detect known strains of ransomware using signatures or patterns. It performs well in the case of existing threats; however, it is ill-suited for new or different form threats. Jain & Rani (2020) noticed that the results of signature-based detection decrease while analysing the modern ransomware payloads and stressed on the necessity of using more adaptive approaches to detection. Singh et al. (2020) also take issue with traditional methods suggesting that although through heuristic analysis, anomalies are identified, they are accompanied by a higher number of false positives since heuristic rules and behaviour patterns are used.

**2. Machine Learning and Deep Learning Approaches**

Recent advancements has seen great improvements in the use of machine learning, and deep learning specifically, to enhance ransomware detection. Alamosa et al. (2021) and Hammadeh & Kavitha (2023) deal with the use of the ML algorithm for the identification of ransomware based on analysed network activity and system behaviours. These approaches incorporate supervised learning to achieve higher accuracy than conventional approaches as they analyze large amounts of datasets in different threats. Zhao et al. (2021) and Wang et al. (2022), build forward to deep learning techniques establishing that the deep neural networks can provide high percentage of detection of new ransomware variants that most of the simpler models often fail to detect because they tend to have a complex pattern. While these techniques counter the problems associated with traditional approaches and call for massive computational power alongside an adequate training dataset.

**3. Network-Based Detection Methods**

Network-based detection methods have come into the forefront due to their ability to analyze traffic patterns with behaviours potentially suggestive of ransomware attack. Software-defined networking and traffic analysis are mentioned by Akbanov et al. (2019a) and Cabaj & Mazurczyk (2016) to illustrate the ways through which ransomware traffic can be detected and data exfiltration attempts. Homayoun et al. (2020) describe frequent pattern mining applied to network traffic for threat hunting which enables one to identify patterns related to ransomware activities. These methods offer an extra layer of detection because they are analysing the behaviour of the network but may be prone to privacy issues and require a continuous feed of traffic data.

**4. Hybrid Approaches**

Hybrid detection methods include integrating two or more sub techniques to enhance the detection ability and also minimize false/positive outputs. Kang & Gu (2023a, 2023b) and Kapoor et al. discuss that a hybrid model of the signature-based, heuristic, and the machine-based technique is ideal because each technique has its advantages. Wang et al. (2023) also stress on the viability of convergence strategies of the two models and the adoption of both conventional and innovative methods to effectively enable the detection system. They are meant to confront the size and the effectiveness of diver’s ransomware viruses, while coming from the position that strength of one method is lessened by the weaknesses of the others. Nevertheless, their application might be problematic and can be computationally expensive.

**5. Forensic and Post-Attack Analysis**

Ransomware analysis and the estimation of actions taken after an event is important to comprehend ransomware and enhance future identification. Boyton et al. (2020) and Davies et al. (2020) stress on forensic analysis to understand the ransomware incidences, presenting the modus operandi and encryption employed in ransomware. In their paper, Mercaldo et al. (2016) pointed out that the understanding of the ransomware’s features can help enhance the detection and prevention procedures. Not only does post-attack analysis contribute to the healing and recovery processes but also the evaluation of current approaches to detection that can be incorporated from the attacks.

**2.10 Ransomware Mitigation Techniques**

Since the creation of ransomware people fighting on the side of protection have made it their mission to come up with better security measures to solve the problem of its diverse types. But the traditors have not stopped here and continued finding new and dangerous vulnerabilities, especially exploiting the ignorance of the general population on cybersecurity, which has kept ransomware active in causing damage. The main strategy of the mitigation has been on how the data that is encrypted by the ransomware can be recovered through reverse engineering or how the ransomware can be stopped from finishing the encryption process fully. However, such approaches do not work in most of the cases: either the users become victims and pay the demanded ransom, or they lose the files forever (Kapoor et al. , 2021). Still, several callable strategies of mitigation have emerged with the chance of enforcing erasures of ransomware and the recuperation of the jammed devices.  
Cabaj and Mazurczyk (2016) used one of them known as the software-defined networking (SDN) that was earlier applied in the decryption of CryptoWall ransomware. This method, however, worked well against other forms too as was evident from the following aspects:- The approach selected was based on blacklisting of the C&C servers during the execution of the sample. Another limitation related to the fact that without the connection to the C&C server, the infected system would not receive the necessary public key for the encryption. While successful, this technique was restricted by the inability of identifying servers that were not categorized as C&C servers. To support this last readjustment two SDN based programs were designed: SDN1 and SDN2. SDN1 concerned with analysing DNS response messages to decide whether the domain already contains the IPs in the blacklist of unauthorised proxies while SDN2 considered the reorganization of the whole network architecture to filter out ransomware activities using OpenFlow protocol.

Another important strategy of mitigation is reverse engineering as seen by Zimba et al. (2018). This method was intended to assess the working principles inherent in different types of ransomwares. By using reverse engineering, the researchers discovered certain features connected to data deletion and data recovery that are clearly inbuilt within the ransomware’s code. It also consisted of several scans like virus scans, obfuscation checks, and meta-data extraction which helped them in identification of various new attributes of ransomware. Moreover, they used sandboxing adenine it allowed to monitor the activity of ransomware on controlled environment. Notably, they discovered that the adversaries often eschewed using secure file deletion techniques thus allowing the researchers to recover the data, especially with volume shadow copies backup at the right time (Hathaliya and Tanwar, 2020).

Baykara and Sekin (2018) introduced the Safe Zone application that stores all the files of the user in a single file and hence prevents external changes. This application maintained the updates of Safe Zone file and other one like File Watcher logged the details of the parent folder and activity going on in Safe Zone. Also, as part of the programme, it was necessary to add a check of the Safe Zone file’s integrity. This system enabled users, not only those with some level of computer literacy but even those who had little knowledge in the same or whatsoever were able to secure their systems and regain their systems to the most recent backup state in the event of a ransomware attack.

**2.11 Summary**

Ransomware has developed from a crude kind of virus to a highly organized criminal activity that is a menace to the global populace. Another factor arising from its morphology is the fact that it can change quickly, together with the fact that it has become more complex to counter in recent times due to the enhanced advancement of its techniques. Lately, ransomware-as-a-service has emerged, which complicates the situation even more, making it possible for more different cybercriminals to deal with it.

Although, there have been improvements in methods for detecting ransomware, such as signature-based, heuristic-based, and machine learning-based methods, obstacles remain because of the polymorphic characteristics of ransomware and new threats’ occurrence. Consequentially, there are instances where the traditional detection methods lag to effectively deal with the new pattern. Also, during the initial steps of an attack, there is little information available to encourage the creation of efficient early warning systems.

Advancements on Mitigation strategies have been directed towards data recovery and prevention of encryption completion. However, the use of these approaches has not been effective as the result of ransomware is continuously evolving. In many cases, software-defined networking appears to be quite effective, yet a sound and integrated case of prevention remains somewhat in the works.

**CHAPTER THREE: RESEARCH METHODOLOGY**

## **3.1 Introduction**

This chapter describes the systematic procedure and tools used to undertake the study on how ransomware is addressed. This chapter also seeks, in as much detail as is possible, to describe the research design, the method of collecting data, data analysis techniques, and ethical issues. This chapter provides the structure for the entire research as it is strong and credible because the whole process is made transparent, replicable, and efficiently conducted. This chapter’s main purpose, therefore, is to describe the data collection technique, namely systematic literature review, and the data analysis technique, namely thematic analysis.

## **3.2 Research Design**

The study design adopted in this research study is qualitative since it is appropriate in the examination of such phenomenon as ransomware. However, the use of qualitative research can enable the identification of the complex and dynamic nature of ransomware threats, the approaches applied in their detection and prevention. As postulated by Creswell (2013), using qualitative research methodology helps in gaining an understanding of the actual experiences, impressions and techniques employed by individuals and organizations in instances of ransomware attack.

The research is aimed at presenting a literature review of the topic. A systematic literature review is a well-planned and very thorough procedure of identifying, evaluating and synthesizing the findings gathered from prior research to answer a research question concerning a particular topic (Booth et al., 2016). This design is consistent with this work as it allows for synthesizing the existing body of knowledge and establish trends, patterns, and identified knowledge gaps in the ransomware literature. To this end, this design entails a normal process of identifying pertinent studies, assessing studies, an synthesize them in an appropriate way to have a defined, in-depth understanding on the topic on hand and thus forming a good basis on which reforms and corresponding mitigation measures can minimally be developed.

## **3.3 Data Collection Methods**

The approach used to collect data in this study is largely secondary research based on a literature search. Babbie (2016) defined secondary data as data that is already existent in the public domain in the form of processed data collected by other researchers, institutions or organisations. secondary data in the context of this research on the detection and mitigation of ransomware are obtained from scientific publications, databases, papers, and other trustworthy sources. For instance, Murti et al (2015) noted that Sources like IEEE, Science Direct and Google Scholar are used to retrieve such literature. This method is crucial in the attempt to procure credible data that would aid the investigation process of ransomware.

A literature review as defined by Fink (2014) is “a systematic, clear, and repeatable approach for finding, analysing, and synthesizing the current corpus of completed and recorded work produced by researchers, scholars, and practitioners”. This position enables the researcher to position his or her study within the academic discourse, making sense of ideas, concepts, procedures, and findings that have been investigated by earlier researchers (Hart, 1998). In this case we adopt the reasoning that getting involved with the existing literature makes it easy for the researchers to expand on the existing knowledge about the subject and hence help in the growth of this field. Further, researchers can select the most suitable methodology by analysing the strengths and weaknesses of various methodologies used in prior research, as urged by Webster and Watson (2002).

Therefore, this study undertakes a literature review with a view of identifying and exploring the phenomenon known as ransomware with a special emphasis on its definition, classification and impacts; and the methods of identification and preventing the attacks. The review starts with the formulation of the research questions; this forms the foundation in the process of searching for the literature so that the review is on track and pertinent. An initial search strategy is proposed; the analysis uses specific search terms and parameters to select the relevant literature. The selected studies are evaluated based on their relevance to the research questions, methodological strength, and the significance of their findings (Ridley, 2012). This makes the results of several studies critical in enabling the evaluation of the quality and reliability of the data obtained. Based on the extracted data, this research offers the current state of knowledge on ransomware detection and mitigation introduced in this work. In the end, the use of only secondary data only from reliable sources make the study expansive and recent enough to serve as a perfect precursor to subsequent analysis.

## **3.4 Inclusion and Exclusion Criteria**

Table 1: Inclusion and Exclusion Criteria

|  |  |
| --- | --- |
|  | Description |
| Inclusion Criteria | **Criteria for Selecting Literature and Data Sources** |
| Relevance | Studies must be directly relevant to ransomware investigation and mitigation, including research on ransomware delivery methods, forensic procedures, mitigation strategies, and related topics. |
| Publication Date | Preference will be given to studies published within the last ten years that is between 2014 to 2024 to ensure the data reflects current trends and technologies in ransomware. |
| Peer-Reviewed Sources | Only peer-reviewed journal articles, conference papers, and reputable industry reports will be included to ensure the quality and credibility of the data. |
| Language | Only studies published in English will be included to ensure consistency in data analysis and interpretation. |
| Exclusion Criteria | **Criteria for Excluding Literature and Data Sources** |
| Irrelevance | Studies that do not directly address ransomware investigation or mitigation, or that focus on unrelated cybersecurity issues, will be excluded. |
| Outdated Research | Research published more than ten years ago will generally be excluded unless it provides foundational or seminal insights that are still relevant today. |
| Non-Peer-Reviewed Sources | Non peer reviewed literature like blogs and news articles that present the author’s opinion as fact, magazine articles and other similar publications that do not follow a highly academic approach will not be used to avoid compromising the quality of the research. |
| Non-English Publications | Only English articles will be included to overcome language difference and possible inaccuracies in translation of articles in other languages which might hamper the judgment and interpretation process. |

## **3.5 Data Analysis Techniques**

The approach that has been adopted in the current dissertation on the identification and combating of ransomware is thematic analysis. As a qualitative approach this method seeks to systematically search, describe or identify, analyze and report patterns or themes within data which makes it suitable for synthesizing secondary data derived from literature reviews (Braun & Clarke, 2006). Thematic analysis involves data identification and reconnaissance, during which relevant research is chosen by preset inclusion and exclusion criteria. A potential advantage of this process is that only high-quality studies are included and information such as the study design and key findings are systemically identify (Kitchenham et al. , 2009). After that, the data is coded and categorized where the researcher involves coding of key concepts or variables either manually or through the help of software [Thomas and Harden 2008]. The researcher then clusters these codes into potential themes that can answer the research questions, hence creating bigger patterns from the data. Last, the results emerging from the analysis of data are compared with the objectives of the study to explain coherently trends, contradictions, or potential gaps with the literature, as well as to propose reasonable hypotheses to justify the phenomena under analysis (Thomas & Harden, 2008). This structured approach also helps to avoid subjective, unfocused and reporting of results with no real analysis.

**3.6 Ethical Considerations**

Even though this study is of the secondary nature, the issues of ethical concern are still critical. The researcher must also make sure that all the sources of the data collected is adequately referenced to avoid any form of plagiarism and therefore infringing on the copyright of the authors (Silverman, 2016).

1. **Proper Attribution**: Any given data and information, which would be incorporated into the study, will be cited to the highest accuracy. This in the view of publications such as research papers, reports, other papers that document facts. This is important to have apart from crediting the original authors, to increase the reliability of the study.
2. **Intellectual Property Rights**: The ethical use of data gathered during the study recognises the copyrights of the authors of the original sources. This includes compliance with any proscribing regulation regarding its use and respecting other’s work.
3. **Sensitivity of Data**: The researcher must be conscious not to disclose the details of the data for public use since the data has to be collected and analysed carefully before being published; this is especially important where ransomware cases are involved and affect real persons or organizations. If there is any information that may be related to any person, organizational unit or related business entity then it will be kept confidential.
4. **Ethical Approval**: Although ethical approval is not normally a prerequisite for secondary data analysis, the researcher should note that he or she may require approval from the local IRB/Ethics committee if the secondary data contains sensitive or confidential data.

By following these ethical considerations, the researcher is able to conduct the study with full compliance with the standards held by the academicians and the contributors of the original data.

**Summary**

Chapter Three provided a description of the research method used in this study which used a systematic qualitative approach to review the literature related to ransomware threat. The type of the study, which is the qualitative research design, coupled with the systematic review, has made it possible to explore the subject matter to its depth because of the complex keep and several side aspects of ransomware that it has been established as having. The method of data collection that has been used extensively in this research is secondary data collection whereby data was collected from credible resources through use of various literature. In this chapter, the criteria that were included when developing a set of guidelines to conduct the systematic review also helped in reducing the studies to only those that are most relevant and of good quality, hence increasing validity of the research. The data analysis was done by thematic analysis; this method is ideal when it comes to coding while looking for patterns of information gathered. This has given a constructive approach in this study in making sure that there is an understanding of the various topics of discussion that revolve round ransomware, its investigation, and avoidance. As for the ethical issues, they have been resolved properly, all the sources were cited, and attention was paid to the use of other people’s material, as well as personal information, that can make a problem in the further work.

# **CHAPTER FOUR: ANALYSIS AND FINDINGS**

## **4.1 Introduction**

This chapter of the study seeks to analyse the data collected on identification and prevention of ransomware in current computer systems. Following the thematic analysis techniques, this chapter investigates the existing detection methods and the measures towards prevention as well as the gaps that are found with the existing frameworks. An analysis of the findings is then made with the aim of understanding the new dynamics of ransomware threats besides the checking of the new improved framework. Pursuant to the analysis of the collected data systematically in this chapter, the researcher has tried to capture a holistic view of the current approaches’ drawbacks and opportunities to pave the way for improved ways to mitigate the effects of ransomware attacks.

## **4.2 Attack Methodology: A Review of the Colonial Pipeline Ransomware Attack**

Specifically, the incident with the Colonial Pipeline can be regarded as an example of a typical structured and systematic approach that hackers tend to use. This section aims at describing the pattern of the attack in the following sub-sections; the common stages in hacking operation, method employed by the DarkSide group, and the lastly, the actions and reactions of Colonial Pipeline Company and the U.S. government. It is therefore imperative to comprehend the various time-based phases in such an attack so as to formulate an adequate defensive mechanism.

**Phases of the Attack**

There are three major steps that are usually in hacking processes through which attackers are able to penetrate into a target system and , thereafter, maintain themselves and achieve their goals. Geeks For Geeks (2023) identified phases of these steps which are reconnaissance, scanning, gaining access, maintaining access and finally, covering the tracks. Speaking of the Colonial Pipeline attack, it is reasonable to assume that the DarkSide hacker group began with good reconnaissance. This phase concerned themselves with identifying the status within the Colonial Pipeline Company about security. For instance, they could have been tracking the employee list on LinkedIn and seeing gaps within the company such as people leaving the company soon (Geeks for Geeks, 2023).

Figure 5: Phases of ethical hacking



(Geeks For Geeks 2023)

Following reconnaissance, DarkSide likely moved on to scanning, where they would have identified open ports and potentially vulnerable accounts within the Colonial Pipeline's network. The next step involved gaining access, which was achieved by exploiting a VPN account that was no longer in active use following the retirement of a company employee. Although the exact method by which DarkSide obtained the password remains unknown, theories suggest possibilities ranging from keylogging to involvement from a disgruntled employee. Ultimately, the password was discovered in a batch of leaked credentials on the dark web (CyberTalk, 2021; GovTech, 2021).

**Exploitation through VPN Access**

Once DarkSide obtained the password, they successfully infiltrated the Colonial Pipeline network through the compromised VPN account. The absence of two-factor authentication on this account allowed the attackers unrestricted access to the entire network. This oversight in security protocol highlights the critical importance of multi-layered authentication mechanisms, particularly for VPN services, which, while effective at blocking external access, become a significant vulnerability once breached (Uberti & Stupp, 2021).

After gaining entry, DarkSide had full control over the network infrastructure, enabling them to execute a chained attack. This involved systematically compromising various systems within the network. The earliest evidence of tampering was detected on April 29, though it is possible that access was gained earlier, allowing the group ample time to plan their subsequent actions. Notably, the hackers maintained their presence on the network undetected for a week, during which they were able to exfiltrate over 100 gigabytes of data (Uberti & Stupp, 2021).

**The Ransom Demand and Colonial Pipeline's Response**

On May 7, at approximately 5 a.m., DarkSide left a ransom note on one of Colonial Pipeline's computer screens, demanding payment of 4.4 million dollars to release their control over the network (Dudley & Golden, 2021). The hackers also threatened to leak the stolen data if their demands were not met. Faced with the potential loss of sensitive information and the crippling of their operations, Colonial Pipeline opted to pay the ransom. This decision underscores the complex considerations that companies face when dealing with ransomware attacks, where the immediate recovery of operational capabilities often takes precedence over the long-term implications of capitulating to criminal demands (Martin & Weiner, 2021; Parfomak & Jaikaran, 2021).

Despite the payment, the full extent of the data theft and the specific methodologies used by DarkSide to cover their tracks remain unclear. The effectiveness of their attack is evident in the substantial ransom payment, the data breach, and the broader impact on Colonial Pipeline's operations and reputation. Moreover, the incident exposed significant vulnerabilities within the company's network, which could potentially be exploited by other hacker groups in the future. As a response, Colonial Pipeline reported that they had switched VPN services to mitigate the initial security flaw that was exploited (Fung & Sebastian, 2021).

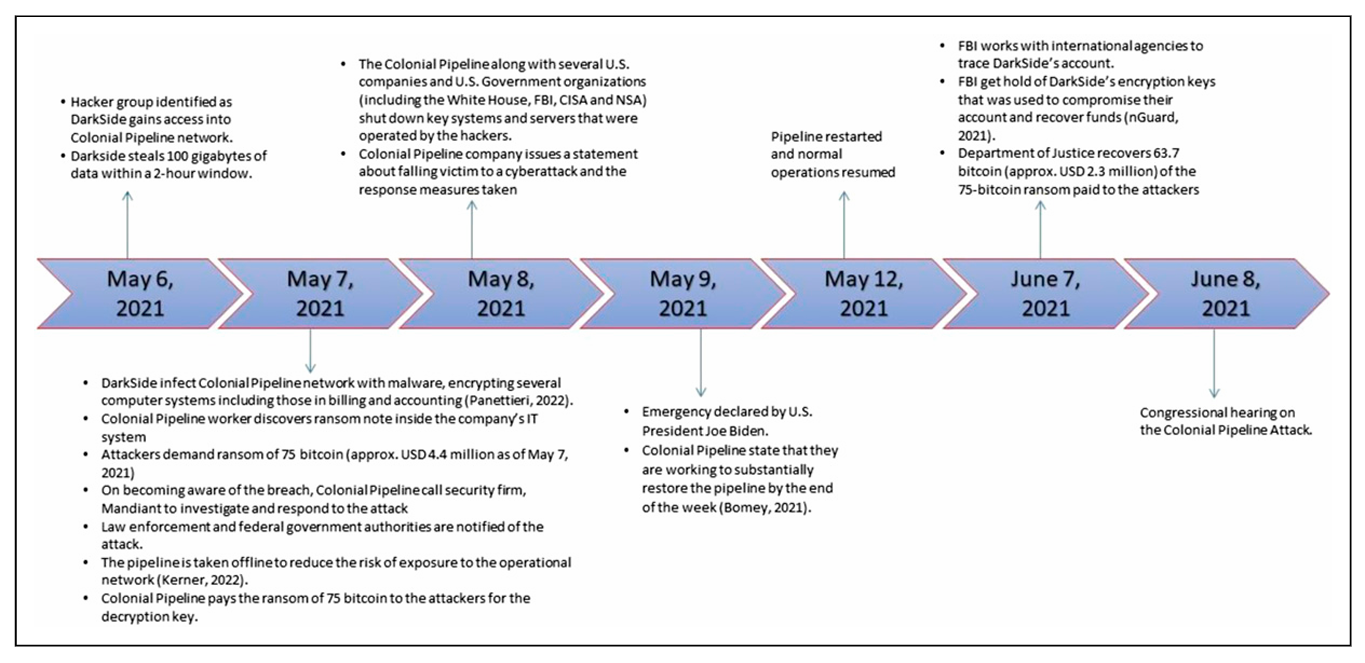
**The U.S. Government's Intervention**

In the aftermath of the attack, the U.S. government took decisive action to mitigate the impact and pursue the perpetrators. The Department of Justice successfully seized $2.3 million of the ransom payment from the DarkSide group. This operation was authorised by U.S. Magistrate Judge Laurel Beeler and executed by the Special Prosecutions Section and Asset Forfeiture Unit of the U.S. Attorney’s Office for the Northern District of California. This seizure, while significant, represents only a portion of the overall ransom paid, and the fate of the remaining stolen funds and data remains uncertain (Office of Public Affairs, 2021).

**Summary**

The Colonial Pipeline ransomware attack serves as a stark reminder of the sophistication and persistence of modern cybercriminals. The methodology employed by DarkSide, from the initial reconnaissance to the final ransom demand, illustrates the critical need for robust cybersecurity measures, particularly in industries that are vital to national infrastructure. The reply of Colonial Pipeline, while forward-thinking, has arisen some concerns and key questions about the lessons that the ransom payments could have on the future agendas as well as the efficacy of the current cybersecurity measures. Since the threat of cyber threats is likely to change, it’s important that new trends in identifying and managing these attacks are put in place. One has to imagine that the lessons learned from the Colonial Pipeline attack should help to guide the further protection of critical infrastructure from comparable threats.

Figure 6: Colonia Pipeline Ransomware Attack Timeline



## **4.3 Evaluation of the effectiveness of current mitigation strategies against ransomware attacks**

To assess the current approaches of mitigating ransomware attacks, there are four main themes identified in the literature and encompass identification, protection and response strategies.

**Detection Techniques**: Ransomware threats have been found to be undetectable by most antivirus programs, and modern detection techniques factor in the identification of ransomware threats greatly. Machine learning methods have come to the foreground in identifying ransomware through the pattern and behavior pattern recognition. For example, Almousa et al. (2021) shows how using machine learning supports the detection of ransomware activity based on analysis of the network traffic data. Likewise, Ispahany et al. (2024) also explores the application of various state-of-the-art machine learning techniques for improving the ransomware detection. Further, Zhao et al. (2021) have come up with a deep learning framework that is tailored to detecting ransomware, the developments in deep learning that show the potential for better accuracy. These techniques are useful in detecting ransomware before they can launch attacks, thus minimizing on the effects to be caused.

**Prevention Strategies:** Prevention continues to be one of the most effective strategies of dealing with ransomware attacks. Measures like often software patching, campaign, and preventive are highly recommended strategies. Bradley (2016) also strongly recommends organisations update their systems as frequently as possible and install security patches to avoid ransomware infecting the system. According to Baykara and Sekin (2018), a “safe zone” concept should develop safe zones capable of dealing with possible ransomwares. In the same study, Wu et al., (2018) presents preventive measures that include behavioural analysis and heuristic based detection mechanisms. These measures are very vital to decrease the incidence of ransomware incidents by proactively focusing on the holes which can be leveraged.

**Response and Mitigation:** What is also important once the ransomware attack has happened is the response including measures that will enhance its mitigation. Reilly (2019) works on varied reaction studies, including the response on the sector level and the response in the context of the healing center industry, sharing the sector viewpoint about the ways to cope with ransomware events. In their article, Ganorkar and Kandasamy (2017) under defensive measures they talk of monitoring and immediate action plan. Further, Prakash et al. (2017) highlights how organisations can approach the framework in terms of incident response Locky ransomware with an effective methodical way of dealing with the issue. These response strategies are useful when it comes to preventing or reducing the extent of damage and carrying out post-attack recovery.

**Advanced Techniques and Future Directions:** The detailed pattern of combating ransomware also affects by the new technologies and techniques from time to time. For instance, the incorporation of federated learning for ransomware detection proposed by Koike et al. (2024) is considered as a more innovative way of developing detection mechanisms through learning within different organizations. Likewise, the study by Singh et al. (2020) on ransomware analysis, and defence also shows that the progress to study ransomware attacks and protect against continues apace. These innovations point to a tendency towards more polymorphic approaches which are essential when trying to counter ever more complex ransomware strategies.

Table 2: Thematic analysis of the evaluation of the effectiveness of current mitigation strategies against ransomware attacks

|  |  |  |  |
| --- | --- | --- | --- |
| Theme | Sub-theme | Key Points | Literature Citations |
| Detection Techniques | Machine Learning | Utilizes pattern recognition and behaviour analysis to identify ransomware. Approaches include network traffic analysis and deep learning frameworks. | Almousa et al. (2021), Zhao et al. (2021), Ispahany et al. (2024) |
| Prevention Strategies | Regular Software Updates | Emphasizes the necessity of keeping software and systems updated to close vulnerabilities that could be exploited by ransomware. | Bradley (2016) |
|  | User Education | Involves training users to recognize phishing attempts and other ransomware delivery methods to prevent infections. | Wu et al. (2018) |
|  | Isolated Environments | Uses "safe zones" or sandbox environments to contain and mitigate ransomware threats before they affect the broader system. | Baykara and Sekin (2018) |
| Response and Mitigation | Incident Response Protocols | Includes real-time monitoring, structured response frameworks, and sector-specific approaches to manage and recover from ransomware attacks. | Reilly (2019), Ganorkar and Kandasamy (2017), Prakash et al. (2017) |
|  | Real-Time Monitoring | Involves continuous surveillance of network activity to detect and respond to ransomware attacks swiftly. | Ganorkar and Kandasamy (2017) |
| Advanced Techniques | Federated Learning | Applies collaborative learning methods across multiple entities to enhance detection capabilities and adapt to new ransomware variants. | Koike et al. (2024) |
|  | Behavioural and Heuristic Detection | Combines behavioural analysis with heuristic methods to identify ransomware based on its actions and characteristics. | Wu et al. (2018) |
| Emerging Trends | Ransomware Analysis | Ongoing research into new ransomware strains and defensive techniques to improve the overall effectiveness and adaptability of mitigation strategies. | Singh et al. (2020) |

## **4.4 Identifying gaps and limitations in the existing detection and mitigation frameworks.**

To conduct a thematic analysis of the existing detection and mitigation frameworks for insider threats, it is vital to ensure that the recurring themes, gaps and limitations evidence from the literature are pinpointed. This analysis will focus on the following key themes:

**1. Technological Frameworks and Their Shortcomings**

The technological methods on insider threat detection and prevention have been the subject of many studies, the most common of which are machine learning, behavioural analysis, and system monitoring tools (Hald & Pedersen, 2021; Probst et al. , 2020; Schultz, 2021). But the frameworks in the same often encounter challenges such as false positives and expensive to implement (Greitzer et al. , 2018; Park et al. , 2021). Despite investments made to improve the technology to identify various insider threats, these technologies often have issues of either low true positive rates or high false positives (BaMaung et al. , 2018). This implies a void in approaches that are implementable across different contexts without compromising on the ability to detect latent cases.

**2. Human Factors and Organizational Culture**

Despite insider threat being a complex phenomenon, end-user behaviour and organisational culture are some of the aspects that are not well researched in most frameworks (Nurse et al. , 2019; Ponemon Institute, 2022). While several researchers agree that organisations’ detection systems do not do an effective job of capturing the details of employees’ behaviour or the potential impact of organisational culture (Shaw & Fischer, 2020). For example, behavioural characteristics associated with stressed employees or those with some sort of grievance may be perceived as suspicious behavior thus creating cases of false positives (Costa et al. , 2019). This points to a major deficiency in applying psychological and sociological findings into detection models, which, when utilised, can help in unveiling the insider’s objectives and increase the preciseness of detection.

**3. Policy and Governance Limitations**

Another highly important area in the literature is the policy and governance involved in the countermeasures of the insider threats. As mentioned earlier, it is a common practice for many organisations to set up policies, but the strength and implementation of these policies are however questionable (Cappelli et al. , 2016; Colwill, 2009). According to the literature, there is a common call for reporting stronger governance frameworks that are defined and sufficiently versatile to accommodate the new threats’ pattern (Gheyas & Abdallah, 2016). Furthermore, there is a concern that there are inadequate broad inflections of a policy-national type which appropriately addresses technical, human and organizational demands (Hunker & Probst, 2011). Such a gap can justify the need for an overall policy that will incorporate all other measures of mitigation.

**4. Data Privacy and Ethical Considerations**

This brings issues such as the conflict between efficient insider threat identification on the one hand and personal privacy of data on the other hand. Several frameworks proposed over the years have been argued to be problematic since they may violate the privacy of the employees or even put the organization in an ethical predicament (Greitzer & Hohimer, 2016; Gaikwad & Chugh, 2021). From the literature, several concerns have been forwarded showing that there is a lack of frameworks that can make it possible to monitor the activities of computer users while, at the same time, respecting their privacy rights (Brackney & Anderson, 2004; Martin & Rice, 2011). This issue is becoming more acute nowadays due to growing popularity of highly invasive monitoring technologies that go beyond simple tracking of user activity and penetration into individual data.

**5. Insider Threat Awareness and Training**

Despite the availability of sophisticated detection tools, the insider threat research reveals that the insider threat detection is not only possible, but many companies have reported that they can detect insider threats (Cole & Ring, 2006; Greitzer et al., 2010). But unfortunately, there is a record of a low efficacy of such programs although many of them may not be organization-specific or fail to adapt to newer issues (Keeney et al. , 2005; PWC, 2021). This implies that an active and consistent training program should be in place, which should be in line with the current and the likely future threats with negative impact on an organization and its security; this will ensure that the workers are able to identify as well as to mitigate the impacts of insider threats successfully.

Table 3: Thematic analysis to identify gaps and limitations in existing detection and mitigation frameworks for insider threats

|  |  |  |  |
| --- | --- | --- | --- |
| Theme | Description | Gaps/Limitations | Key Literature |
| Technological Frameworks | Focuses on the use of machine learning, behavioural analytics, and monitoring tools for detecting insider threats. | High false positive rates  High implementation costs  Limited real-world applicability  Balance between accuracy and usability is lacking | Hald & Pedersen (2021); Probst et al. (2020); Schultz (2021); Greitzer et al. (2018) |
| Human Factors and Organizational Culture | Examines the role of employee behaviour and workplace culture in insider threat scenarios. | Insufficient integration of psychological and sociological insights  Lack of understanding of employee motivations  Potential for false positives | Nurse et al. (2019); Shaw & Fischer (2020); Costa et al. (2019) |
| Policy and Governance | Discusses the role of organizational policies and governance frameworks in mitigating insider threats. | Inconsistent enforcement of policies  Lack of comprehensive and flexible governance frameworks  Poor integration of technical and organizational aspects | Cappelli et al. (2016); Colwill (2009); Gheyas & Abdallah (2016) |
| Data Privacy and Ethical Considerations | Addresses the balance between effective threat detection and the preservation of employee privacy and ethical standards. | Potential infringement on employee privacy  Ethical dilemmas due to invasive monitoring  Lack of frameworks balancing monitoring and privacy rights | Greitzer & Hohimer (2016); Gaikwad et al. (2021); Brackney & Anderson (2004) |
| Insider Threat Awareness and Training | Focuses on the importance and effectiveness of awareness and training programs for mitigating insider threats. | Ineffective or outdated training programs  Lack of contextualization for specific organizations  Failure to evolve with emerging threats | Cole & Ring (2006); Greitzer et al. (2010); Keeney et al. (2005); PWC (2021) |

## **4.5 Mitigation Techniques in Ransomware Attacks: Colonia Pipeline**

This research addresses the understanding about effectiveness of mitigation techniques to prevent and contained ransomware attacks for any organization. These attacks, that have increasingly become common in recent years, present certain threats to businesses and if not handled well can cause much havoc in an organization. According to Bullock et al. (2013) mitigation entails effort to minimize and/or prevent loss of life and property due to hazards and impact. As can be seen in the case of ransomware, suitable measures are necessary to minimize the effects of the attack, and to restore normal functioning of the company’s activities as soon as possible. It is best practiced early on as the tactics that the attackers use is gradually becoming more and more complex.

A major preventive measure of ransomware entail computers and networks should be properly installed and maintained. It is a prerequisite that these systems should be properly configured, and this is the only way to avoid attacks. For example, Operating system, application software, web browsers, plug-ins, firmware ones and anti-virus software should be updated. Such updates should be well and extensively examined and it should be done in a way, which will not bring new threats to the system (Singh & Sittig, 2016). Also, network engineers should ensure that organisational firewalls are configured well to deny unauthorised form of access to resources. Some of these fundamental security practices are the primary level of defence against ransomware and, if practised, will dramatically lower the risk of this threat.

Beyond the technical aspects, the organisations should also employ control access polices. These policies would limit the rights of the user to write new files and delete files from computers as well as install and execute application software and access only the systems and services relevant to their job specifications. There is a principle known as “Least Privilege”; it helps in reducing users’ access rights to everything concerning their roles and expectations in the organization (Singh & Sittig, 2016, p.58). For users who require administrative privileges, organisations can create two accounts: the first one with administrative privileges for certain purpose and the second one with limited privileges for performing routine job such as reading a mail or searching on the world wide web. These practices assist to reduce the consequences of ransomware attacks through reducing the activities that users can undertake within the network.

In enforcing ransomware defense measures, other activities where technical defense and access controls are vital are security awareness training. Training should be educative as well as fun to help express the knowledge relevant in detecting and combating possible dangers. This kind of training must be conducted since even the best technical defense mechanisms are sometimes breached by human factors. External security awareness training frameworks can also be adopted meaning that the organisation does not have to come up with new content from scratch. The IT staff should discuss the layers of attacks with the users during these sessions to develop proper scenarios that will challenge them (Singh & Sittig, 2016). For instance, IT staff may assist the users to differentiate between a genuine e-mail and a fake one by sending examples of e-mails from IT department of the organisation. This creates rapport between the IT team and the users and therefore improves the outcome of phishing detection.

In addition, engaging in such measures as sending out fake phishing emails and carrying out bogus system backup drills will help heighten the users’ countermeasures readiness against future ransomware attacks. The readiness can also be tested by Feeding wrong emails or links that seem to be replicated from legitimate sources and this will assist organisations in training the users while at the same time building capacity (Singh & Sittig, 2016). These exercises are very useful and vital so that the users can be more alert to fraud so that they can report any suspicious activity. All accounts of the application incorporate two-factor authentication which enhances the level of security and makes it more difficult for an attacker to get access to another user’s account.

Another key component of ransomware risk management is the need to supervise potential suspicious activities. The reliable network and user activity monitoring system can identify incipient signs of an attack to prevent their execution such as emails from the known fraudulent addresses, executable file e-mail attachments, modifications of the keys, unknown processes compiling the files, sharp growth of network traffic in the unknown ports (Singh & Sittig, 2016). The efficiency of the programme guarantees quick response to threats, which significantly decreases the consequences of a ransomware attack in the organization. Apogee thus proposes that IT staff carry out a frequent check on the external environment to ensure that the identified risks are still present hence making sure that the implemented risk control continues to be as effective as when it was first put in place.

In the event of a ransomware attack, users must know the appropriate steps to take to protect themselves and the organisation. If an attack occurs, affected users should immediately turn off their computers and report the incident to the IT support team. IT professionals should then disconnect the infected machines from the network and disable wireless network functionality to prevent the spread of the ransomware. In cases where the attack becomes widespread, both wireless and wired networks should be shut down to contain the damage (Singh & Sittig, 2016). These precautions are vital for an organisation's survival in the face of increasing security threats. Furthermore, organisations should collaborate with external security experts to continually assess and enhance their systems and security policies.

The Colonial Pipeline ransomware attack in May 2021 serves as a stark reminder of the importance of robust mitigation strategies. This attack, which disrupted fuel supplies across the eastern United States, highlighted several areas where improvements could have been made. If the Colonial Pipeline system had been better secured, particularly using multi-factor authentication, the attackers might have been less likely to gain access to critical systems (Medlock III, 2021). Strong passwords, anti-malware software, and vigilance against suspicious links are basic but effective methods that could have helped mitigate the damage (Monteith, 2016).

In response to the growing threat of ransomware, the United States government has taken steps to strengthen its defences. The Department of Justice (DoJ), for instance, has established a Ransomware and Digital Extortion Task Force. This initiative was introduced to combat the rising number of cyber-attacks targeting the nation’s critical infrastructure, including the Colonial Pipeline attack (DeMarco, 2021). One significant measure undertaken by the DoJ was the issuance of a memorandum by Deputy Attorney General Lisa Monaco on 3 June 2021. This memorandum instructed federal prosecutors to treat ransomware cases with the same urgency and seriousness as terrorism cases, centralising the tracking and handling of these incidents (DeMarco, 2021). Such an approach underscores the critical importance of ransomware mitigation at both organisational and national levels.

## **4.6 Proposed Detection and Mitigation Framework**

Based on the thematic analysis and identified gaps in the literature, the following is a proposed enhanced, comprehensive framework for the detection and mitigation of ransomware. This framework integrates multiple layers of defence, focusing on early detection, proactive prevention, user education, and standardized response mechanisms.

**1. Multi-Layered Detection Mechanism**

**a. Signature-Based Detection:**

* Continue to utilize signature-based detection for identifying known ransomware strains. This method remains effective for detecting previously catalogued threats with established signatures.
* **Integration:** Behavioral analysis systems should be complemented in parallel to update the current signature databases in a bid to detect new variants.

**b. Behavior-Based Detection:**

* Integration of machine learning algorithms that study behaviours of users and the system to identify behaviours associated with ransomware. This could include watching out for encryption settings on files, abnormal access attempts on files or even processes’ behavior.
* **Hybrid Approach:** As an approach, behavioural detection should be used in conjunction with signature-based techniques to minimize false positives. For example, if an anomaly is detected, then the signature analysis would be done before an action is taken.

**c. Anomaly Detection Using AI:**

* Utilise machine learning models that can be trained with past data and act in response to emergent threats in real time. These models should be capable to learn with new methodologies of ransomware, and to shorten the time between detection of this threat and the appearance of new types of ransomwares (Sgandurra et al. , 2016).

**2. Proactive Threat Intelligence Integration**

**a. Threat Intelligence Feeds:**

* Include threat intelligence feeds that contain timely data such as newly developed ransomware threats, blacklisted IPs and domains.
* **Pre-Attack Detection:** Learn from this intelligence to detect a possible attack prior to staging entry in the network, primarily through the usage of the blocking method in the known evil entities (Al-Rimy et al. , 2018).

**b. Honeypots and Deception Technology:**

* Set up honeypots intended for ransomware that would lure in such attacks and bag which can be used in learning better ways of how to detect such threats and prevent their execution.
* **Information Sharing:** Data collected in honeypots must be forwarded to other platforms to feed global threat datasets (Griffin et al , 2019).

**3. User Education and Awareness Programs**

**a. Phishing Simulation and Training:**

* Exercise the users frequently through simulation phishing to let them know the risks that are associated with ransomware such as email with attachments or links to some sites.
* **Behavioural Metrics:** They should monitor the reactions of users to those simulations to capture high-risk attendees that may need more training (Taylor et al. , 2019).

**b. Incident Response Protocols:**

* Implement and educate personnel on certain practical measures in case of probable ransomware attacks such as disconnecting the contaminated machines and informing the technology teams.
* **Automated Alerts:** Use notifications that will ensure that the user is informed on steps to take when a ransomware is identified.

**4. Standardization and Interoperability**

**a. Unified Defense Framework:**

* Implementation of best practices to be followed consistently to the different platforms and security tools used in the detection and prevention of ransomware.
* **Industry Collaboration:** A security vendor should foster integration of systems, where products made by different security vendors should collaborate through integration by means of API and data sharing standard that allows different security systems to work in an integrated manner (Kharraz et al., 2016).

**b. Centralized Monitoring and Reporting:**

* Ensure that deployment of network based security tools that are used for monitoring of security events/systems are integrated in a single common platform.
* **Automated Correlation:** Intensify the integration of automated systems to correlative several data sources to boost the identification of intricate multi-vector ransomware attacks (Kolodenker et al. , 2017).

**5. Post-Attack Mitigation and Recovery**

**a. Regular Backups and Redundancy:**

* Purge all unessential files from local databases and back the copies of received and sent messages, customers’ records, account information, and other important data, at least once a week, in encrypted form, at different locations that can be used to restore lost data as soon as possible in case of the ransomware attack.
* **Immutable Backups:** Employ ‘write once, read many’ or WORM type back up that cannot be modified or erased by ransomware as stated by Scaife et al. , (2016).

**b. Rapid Incident Response Teams:**

* Formulate teams with well-defined responsibilities in handling particular types of cyber mishaps, particularly ransomware ones. Such teams should have equipments for containment of the problem, restoration of the systems and diagnosis in case of future incidence.
* **Forensic Analysis:** Post-incident, take time to investigate the attack mechanism to identify where the vulnerability of the system laid before modifying this detection mechanisms.

**6. Legal and Compliance Considerations**

**a. Compliance with Industry Standards:**

* Ensure that the framework complies with a set of rules and practices characteristic of some industry, for example, GDPR for the EU’s data protection or NIST practices for cybersecurity.
* **Regular Audits:** Carry out checkpoint regularly that will enhance compliance and help in the detection of any vulnerability in the ransomware mitigation strategy (Taylor et al. , 2019).

**b. Legal Readiness:**

* Establish various legal procedures to be followed when dealing with ransomware attackers, especially on the use of law enforcement and the procedures for making the ransom payments, if any.
* **Data Privacy Considerations:** It has to be ensured that the legal response also factor in data privacy laws and risks involved in data breaches due to ransomware.

**7. Continuous Improvement and Adaptation**

**a. Ongoing Research and Development:**

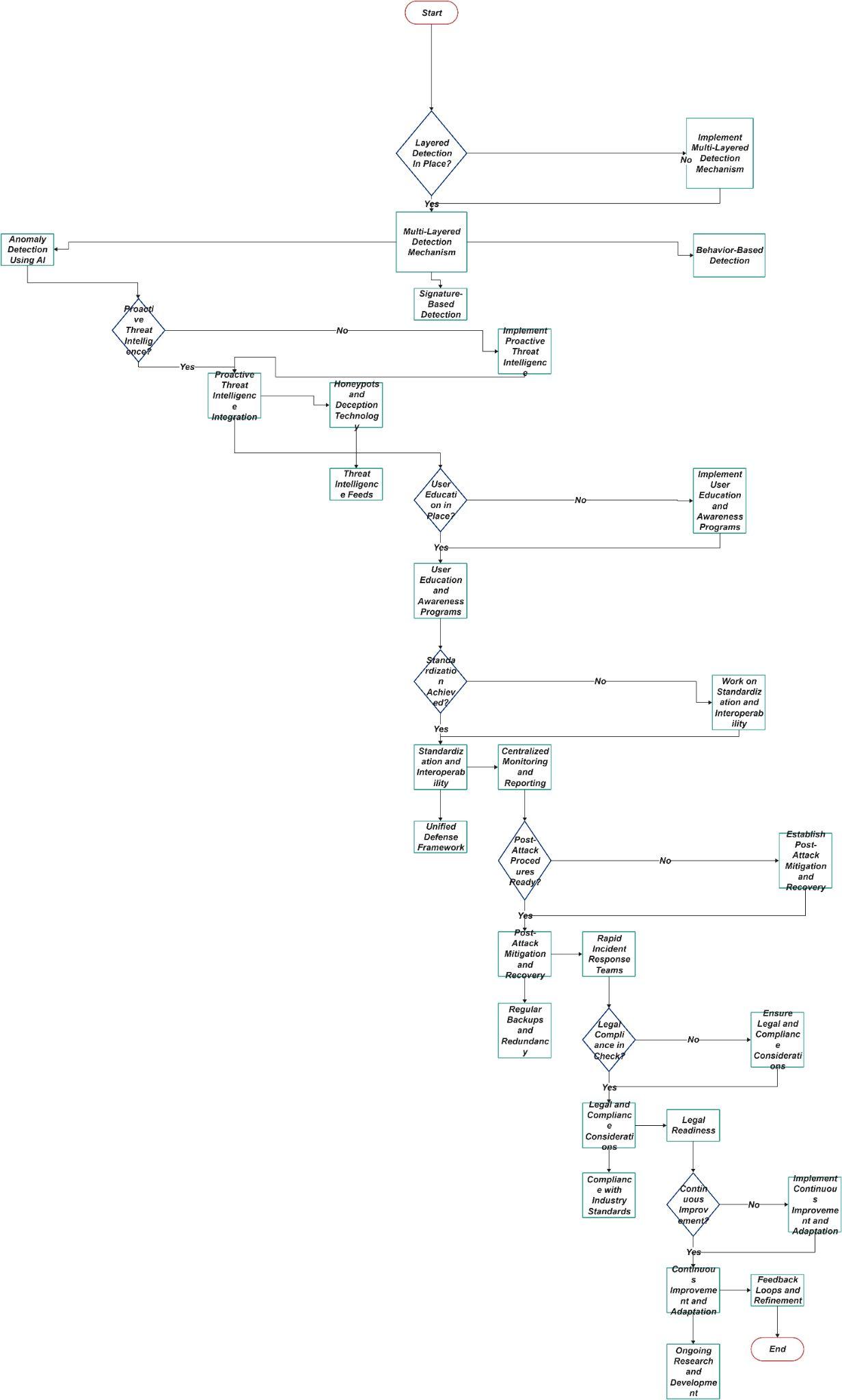
* Continued research should be conducted to regularly update the framework with new ransomware threats and ways of preventing attacks.
* **Community Engagement:** Participate with the larger cybersecurity community to collaborate on the identification of ransomware and with the aim of sharing effective countermeasures, measures or tools (Griffin et al. , 2019).

**b. Feedback Loops and Refinement:**

* Setting feedback loops from all the layers of the framework to enhance and update the layers as more performance data and new threats arise are discovered.
* **Periodic Review:** Reviewed and updated every now and then in response to the emerging challenges and integration of technology options (Sgandurra et al. , 2016).

"This conceptual model focusses on giving high level of protection against ransomware threats by filling the mentioned gaps and using multiple facets to implement the preventive measures, early detection, active involvement of users, and continual reassessment This model presents a robust platform to the ever-evolving spectrum of ransomware threats.”

## **Proposed Ransomware Detection and Mitigation Framework’s Flowchart**



## **4.7 Summary**

Chapter Four of the research deals with the analysis and findings of the study on detection and mitigation of ransomware with the case of Colonial Pipeline ransomware attack. The chapter explains how, DarkSide group used a sequential attack strategy in attacking the company as shown in the following subtopics: reconnaissance and exploitation by exploiting the company VPN and finally the ransom. The study then assesses the current approaches for detecting and preventing ransomware attacks, with focus on machine learning, software updates, and user awareness. Moreover, the chapter outlines weaknesses of existing frameworks, for example, technologies; people; and policies. The adequacy of the mitigation measures is also considered with an emphasis made on the security measures, access controls and the training of the users. Last but not the least; the chapter ends with the discussion of the potential update of ransomware defense tactics due to dynamic threats.

# **CHAPTER FIVE: SUMMARY CONCLUSION, RECOMMENDATION AND SUGGESTION FOR FURTHER STUDIES**

## **5.1 Introduction**

This chapter summaries the overall of the dissertation and give the overall conclusion, recommendation on how to detect and mitigate ransomware based on the finding of the dissertation, and then proposal for further study were also made.

## **5.2 Discussion of Findings**

The subsequent analysis of the Colonial Pipeline ransomware attack provides important information about the general pattern of ransomware detection and risk management. The findings can be seen as greatly corresponding to the research objectives; they specify the advantages and the drawbacks of the existing strategies and suggest which areas might be further improved.

**Comprehensive Assessment of Existing Ransomware Literature**

The Colonial Pipeline attack shows that ransomware threats have become more advanced more complex, and cybercriminals are changing their strategies. This case reveals the trends identified in the more recent ransomware articles, namely, careful planning and selection of the target, as well as the speed of the attack. The case where an organization’s VPN account was compromised, and there was no multi-factor authentication, is seen to be an insecurity common with many ransomware attacks. The literature, as is evident again and again, stresses the necessity of having multiple and deep layers of security to combat such loopholes.

**Evaluation of Current Detection Techniques**

Ransomware identification still poses a significant problem in today’s computing networks. The Colonial Pipeline attack example shows the lack of immediate detection solutions, especially the methods that can be used to indicate the presence of an attacker in a system before they cause extensive harm. A review of literature reveals that machine learning and deep learning approaches can accurately detect abnormal behaviour associated with ransomware. Still, the recent Colonial Pipeline attack proves that these techniques should be incorporated more seamlessly into the organizational security model to prevent threats from developing further.

**Assessment of Mitigation Strategies**

The measures taken during the Colonial Pipeline attack are also the strengths and weaknesses of the existing approaches. Although the organization was able to regain control of their network later, the first reaction giving in to the attackers’ demands stems from the incident desperation. This decision also raises questions as to effectiveness of other mitigation measures that have been used previously since they may not be enough to warrant such measures. The literature reveals that approaches of software patches, user awareness, and access rights are critical but ineffective to guard against elaborate schemes as the attack on Colonial Pipeline. The attack highlights the need to implement and integrate the latest technologies, which are like multi-step verification, constant network scanning to boost the security of systems against ransomware.

**Identification of Gaps and Potential New Methods for Mitigation**

The incident at the Colonial Pipeline has brought into light several limitations associated with the currently available risk mitigation strategies. First, due to the absence of effective solutions for real time detection and prevention, the attackers were able to operate within the network without being detected for an unusually long time. Also, the lack of proper MFA and strong password practices hampered the company which led to the success of the attack. These gaps point to possible new ways of preventing ransomware such as the need to research and implement better methods of authentications, better systems of monitoring in real time, and more intensive training of users in how to identify and how to handle ransomware threats.

**Proposal for a Framework for Detection and Mitigation**

Based on the limitations that have been found in the Colonial Pipeline case and other studies, a number of recommendations could be derived for the detection and prevention of ransomware attacks. This framework should include multiple layers of defence solutions which include machine learning and deep learning for early detection and strong authentication solutions to prevent any form of intrusion. Furthermore, user awareness and simulation should be carried as a constant activity in this framework, so that every employee is able to identify possible threats.

## **5.3 Conclusion**

Due to this rationale, Ransomware has evolved into a highly sophisticated and formidable entity. Today where the attackers are constantly adapting their strategies while exploiting any available weakness. The findings from this dissertation highlight a harsh reality: that there has been progress, but the current frameworks lack certain capacities important for management and must be addressed as soon as possible. This paper aims at analysing the Colonial Pipeline attack and show how it revealed systemic weaknesses in cybersecurity. Even though the organizations have lots of resources and access to sophisticated technologies, the attack was successful because of the lack of fundamentals including not setting up MFA on a VPN account. This example clearly illustrates how even insignificant problems can be used by the attackers to launch very dangerous and profound attacks, which underlines the necessity to develop and implement much more stable and effective security systems.

The current methods used in the detection of threats, as much as they are sophisticated are not all efficient. In reacting to threats, signature-based approaches are appropriate for known threats but are poor against new ransomware versions. Machine learning based behavior analysis is quite effective, but more research needs to be done to minimize false positive rates that are usually associated with this method. There is promising signs of AI and deep learning in being able to adapt to new threats as seen in this paper, however these technologies need to advance more rapidly if they are to become a match for the advancing sophistication of ransomware. Prevention is essential in dealing with the problems, but the principles laid down for it are not well practiced. There is a need to update the software, to train the users, and to prevent the systems; but many organizations do not sustain these practices at the right level of diligence. Using a ‘safe zone’ approach to prevent ransomware is an interesting concept; however, it requires more organizations to embrace it and implement it in real life to make a real difference.

Unfavourable response to ransomware attacks reveal some aspects in it that requires enhancement. Present-day incident response frameworks differ in their efficacy and many organizations fail to have the means to respond to an attack fast and effectively. Real time monitoring needs to be used, frequent simulations carried out and detailed recovery plans need to be created which are always lacking. There is dire lack of specialized teams for handling such incidents and increase legal preparedness such as elaborated guidelines on how to proceed with the ransom demands or data breaches. Some of the problems that have been seen it that there is a missing link in how technology is implemented and human interaction. Even though many frameworks focus on technological mitigation strategies, there is little attention paid to the psychological and sociological dimensions of ransomware risks. Knowledge of human behavior and culture along with factors like stress or employee grievances in affecting security practices can go a long way in enhancing the detection and response capabilities of an organization’s security team.

However, measures need to be taken to enhance policy and governance related frameworks. Secure policies require strict enforcement with the option of adjusting to the emerging threats during the implementation. The same can be said with comprehensive monitoring and data privacy because while the former promotes an efficient protection, the latter respects the rights of an individual. Thus, to fill the identified gaps, the proposed comprehensive framework constitutes a complex, multi-perspective approach to ransomware risks’ identification and prevention. This work proposes a framework that embraces the sophisticated detection mechanisms, threat intelligence, user awareness, best practice, and detection, and constant adaptation so that there will be improved methods to fight the ransomware attacks. That is why it stresses more on a strategy that brings about change in technology accompanied by change in culture, policy, and law. Finally, the problem of ransomware is not one that may be solved sporadically with disjointed solutions or in small increments with numerous optimizations. Real world complexity demands a collective effort to respond to the identified threats and risks which exist, and new ones which emerge during the process, as well as to improve the strategy as it progresses. The findings from this dissertation highlight the urgency of this ongoing battle and the need for a unified, comprehensive approach to safeguard against the ever-evolving threat of ransomware.

* 1. **Recommendations**

The following recommendations were made based on the insights and findings of the study

**Enhanced Multi-Layered Detection Systems**: It is advisable for organisations to use the latest machine learning and AI-based IDSs that use both; the signature-based and the behavior-based techniques. This works well in enhancing the detection accuracy of ransomware by eradicating frequent false positive incidents and flexibility as it addresses new variant of ransomware. Also, frequent updating of signature databases used and behavioural analysis models used in such systems are important. These resources are updated with the latest threat intelligence to help in the early identification of any new ransomware risks.

**Strengthened Proactive Prevention Measures**: Design and stick to frequent patching/update schedules for the operating systems, the software applications, as well as firmware. This makes them less prone to attacks that ransomware maybe ,could capitalise on. Implement MFA to all programs of an organization especially the sensitive areas such as the Virtual Private Network.

**Comprehensive User Education Programs**: Continuously practice phishing tests or quiz like activities and computer-based training programs to remind the employees of current threats and increase their capability to identifying potential ransomware attacks. Ensure that employees read or listen to scripts of comprehensive contingency plans of action to be followed once a ransomware has been identified. It is important to see that these protocols are made current and rehearsed.

**Robust Incident Response and Recovery Planning**: Establish specialized incident response teams of professionals that are well equipped with the responsibility of dealing with ransomware attacks. Provide such teams with the appropriate equipment for holding, restoration, and investigation. Perform backup of certain data sets that are encrypted in a routine manner as well as make sure several copies are taken to different locations. Adopt rigid backup systems to avoid any changes or deletion by ransomware.

**Strengthening Legal and Compliance Frameworks**: Ensure compliance with industry-specific regulations and cybersecurity standards, such as GDPR or NIST. Regularly audit policies to identify and address any gaps in compliance. Develop clear legal protocols for dealing with ransom demands, including engagement with law enforcement and considerations for handling ransom payments.

**Ongoing Research and Adaptation**: Check out the compliance with the regulations typical for the specific industries or security standards like GDPR or NIST. It is important to conduct a formal review of policies instituted within an establishment in a bid to ensure that they address adequate compliance problems. Ensure that there is legal guidelines regarding handling cases with ransom demands, how to address them including involving the police and legalities relating to dealing with ransom money.

## **5.5 Suggestions for Further Studies**

1. **Exploration of Emerging Threats**: Invest on empirical research on how ransomware has changed its mode of prevention and methodologies especially on newly developed types of ransomwares. Explore how quantum computing innovates, specifically, to ransomware protection. Discuss possible developments and changes that need to be made in relations to these dangers.
2. **Human Factors and Behavioural Analysis**: Investigate the correlation between human behaviour and organisational culture with regards to cybersecurity. Create partnerships of psychological and sociological theories that may be used to improve on the approaches that detect and reduce fraud incidences. Analyse the effectiveness of user training programs and phishing simulations in the long-term. Determine techniques that can be used to increase the level of awareness and response for ransomware attacks among users.
3. **Integration of AI and Machine Learning**: Subsequently, deep dive into different aspects of AI and machine learning employed in detection of anomaly for ransomware. Examine the effectiveness of various types of AI solutions and their capacity to improve the speed of response to altering ransomware approaches. Consider the applicability of federated learning for threat intelligence sharing and ability to improve the cooperation on ransomware detection and prevention across the organisations.
4. **Economic and Policy Implications**: Compare the economical outcome of ransom payment and other measures of risk management. Investigate the impact of ransom-paying on the organization’s resilience on both the short and the long-term. There are current policies and governance frameworks addressing cybersecurity generally, and or specifically ransomware, Research on their efficacy. It is necessary to come up with the measures that will help to establish stronger and less sensitive policy frameworks.
5. **Global Perspectives and Collaboration**: Research on how global collaboration and intelligence on ransomware work. That is why it is necessary to determine how successful cooperation in interstate space and work on finding the means to improve the level of cybersecurity in the world is possible. Assess how regional disparities in threats or cybersecurity and cybersecurity measures impact ransomware protection. Generate guidelines for further work on the local level to raise the awareness and detection of the ransomware attacks.

Ransomware is a constantly evolving rogue and infiltrating in the most sophisticated ways attackers can think of and therefore the search for accurate detection and prevention is more befitting and important now than ever before. The findings from this dissertation underscore a stark reality: however, the existing frameworks are not free from issues that required special attention and they are still in their infant stages.

These gaps are best illustrated by the recent Colonial Pipeline attack. Even with great financial and technological firepower available to today’s organizations, the attack was possible due to elementary mistakes such as the absence of two-factor authentication of a VPN account and the general flaws in many organizational cybersecurity strategies. This remains a clear indication that amidst every loophole, a malicious attack can be launched, therefore the need for a much more effective and thorough defense.

Modern detection methods though are highly developed are still associated with one flaw or the other. Traditional approaches for instance, signature-based techniques are helpful when dealing with known malware types but fails when new types of ransomwares come into the picture. Behavioural detection and that which utilizes machine learning is one of the most viable approaches, but there is still a long way to go in an endeavour to eliminate false negatives and enhance reliability. The application of AI/information deep in learning to the development has the potential of the future, but these technologies must adapt quickly to the new threats as ransomware becomes increasingly complex.

Preventative measures are still in practice but serve as critical pervasive and still not effectively put into practice. The common measures include making regular software updates, user education, and other proactive system defense – and most organizations fail to keep these approaches in adequate levels of due diligence. The ‘safe zone’ concept employed in eradication of ransomware might work, but the idea needs to be implemented more frequently and tested in real-life scenarios.

Again, the measures taken to respond to ransomware attacks show that there’s still very much room for improvement. The current incidence response frameworks effectiveness is variable since many organizations are not adequately prepared to respond to attacks expeditiously and efficiently. The use of real time monitoring, scheduled drills and clear recovery strategies should be the standard commercial practice however this is often lacking. It cannot be overemphasized that there is a necessity to employ dedicated incident response teams and overall improved legal preparedness as well as specific guidelines for responding to ransom demands and data breaches.

There is a definite gap, which concerns the integration between technological solutions with the human element. What is more, while various frameworks pay much attention to technological aspects of ransomware threats, the psychological and sociological dimensions are left relatively uncovered. Knowledge regarding employees’ behavior, organizational culture as well as stress or grievances’ influence on security work can dramatically improve the detection of threats and response efficiency.

In addition to that, policy as well as governance frameworks require enhancement. What’s more, one would note the importance of policy compliance in relation to security and versatility in the fight against new emerging threats. Both extremes of comprehensive monitoring and the protection of data also present a dilemma because overly protecting data can also be questionable since it limits people’s rights while on the other end, inadequate protection of data presents new threats.

As such, the proposed comprehensive framework provides a framework-based, multidimensional approach in facing the existing and emerging ransomware threats. To achieve a more robust protection against ransomware, this framework is devised to combine sophisticated detection methods, threat anticipation, users’ awareness, best practices, and improvement of the system. It underlines the necessity of an integrated approach to meet the challenge, which cannot be solved solely with the help of technology tools but also requires proper organizational culture, policy implementation and legal regulation.

Ultimately, the battle against ransomware is not a one-person fight or prevent all such incidences by implementing small changes. It takes team work to counter existing threats, respond to new threats and develop new measures for countering threats considering ever evolving threats. This is a constant fight, as evidenced by the results of this dissertation to find ways to address this threat as prevention and combating ransomware as continuously evolving, require a collective effort and a broad strategy.