International Journal of Scientific and Management Research
Volume 8 Issue 6 (June) 2025
ISSN: 2581-6888
Page: 63-108

Investigating The Factors and Impact of Cybercrime on Small-To Medium-Sized Business (SMBs): Analysing risks, factors, and solutions

Ugochukwu Anthony Igboko
IT Analyst, Digital and ICT, South Tyneside Council, **United Kingdom**
DOI - http://doi.org/10.37502/IJSMR.2025.8606

Abstract

This study examines how cybercrime affects small and medium-sized businesses (SMBs) and recommends ways to make them more secure. The increasing prevalence of cyber threats and the vulnerability of SMBs in the current digital landscape highlight the importance of addressing cybersecurity challenges. The study aims to provide a comprehensive understanding of cybercrime against SMBs and develop a practical framework to mitigate these threats.

The research employs quantitative research design with a survey-based approach. A sample of SMB owners, managers, and IT personnel was selected using purposive and stratified random sampling techniques. Data was collected through a structured questionnaire, and descriptive and inferential statistical techniques were used for data analysis. The research methodology ensures the validity and reliability of the findings.

According to the research findings, phishing attacks are the most frequent cyber-threat to SMBs, followed by insider threats. Cybercriminals target servers as their main target, taking advantage of vulnerabilities like outdated software, weak passwords, and a lack of multi-factor authentication. Although preventive measures like multi-factor authentication and routine software upgrades are commonly used, SMBs still face difficulties due to a lack of funding, cybersecurity experience, and resources. These challenges call for recommended solutions which are carefully implemented based on the identified challenges. The study emphasises the importance of considering emerging threats, human factors, cybersecurity regulations, economic impacts, collaboration and information sharing, socio-cultural factors, supply chain risk, evaluation of cybersecurity frameworks, long-term impact of cyber incidents, and the role of automation and artificial intelligence in SMB cybersecurity.

In conclusion, this study provides valuable insights into the factors and impacts of cybercrime on SMBs and proposes a practical framework to enhance their cybersecurity. The research contributes to ongoing efforts to protect SMBs from cyber threats and creates awareness among policymakers, industry practitioners, and researchers about the specific challenges faced by SMBs in the digital landscape. Implementing the proposed framework can help SMBs strengthen their cybersecurity resilience and mitigate insider threats. Future research in the identified areas can further enhance the understanding and support SMBs in navigating the evolving cyber threat landscape

Keywords: UK council, Healthcare, SLR, cyber resilience.

1. Introduction

1.0 Background

Cybercrime, a widespread concern in the modern digitally interconnected society, poses a significant threat to both individuals and corporations alike (Fahlevi et al., 2019). Small and medium-sized enterprises (SMEs) are inherently susceptible to cyber threats due to their limited resource allocation and comparatively limited exposure to the realm of cybersecurity. According to a survey conducted by the Better Business Bureau (2020), it has been determined that cybercrime inflicted a collective financial loss of approximately £12.7 million upon small and medium-sized businesses (SMBs) in the United States during the year 2019.

This compelling statistical data underscores the imperative nature of comprehending the underlying factors contributing to cybercrime targeting SMBs, as well as its consequential ramifications on their operational dynamics (Frank et al., 2022). Small and medium-sized businesses (SMBs) are susceptible to financial setbacks stemming from incidents such as cash misappropriation, ransomware infiltrations, and revenue depletion due to disruptions in their operational systems. The detrimental consequences of cyber-attacks extend beyond mere financial implications, encompassing the decline of a company's reputation and the subsequent attrition of its customer base, strategic alliances, and supply chain networks (Frank et al., 2022).

Any illegal activity that utilises the Internet or other computer networks is referred to as "cybercrime." Cybercrime has been more frequent and severe in recent years, affecting both individuals and organisations of all sizes (Perwej et al., 2021). For instance, 40% of firms in the United Kingdom (UK) reported cyber security events in 2022 (AAG, 2023), most likely as a result of the pandemic, according to the UK Cyber Security Breaches Survey (Johns, 2021). Each organisation typically suffers £8,460 in financial loss as a result of these accidents. According to the Canadian Survey on Cyber Security and Cybercrime, 21% of all businesses experienced cyber security issues in 2019 (Statistics Canada 2020). This, for instance, had an impact on 29% of companies with between 100 and 500 employees as well as 18% of organisations with fewer than 100 employees. Due to their limited financial resources and lack of cybersecurity expertise, small and medium-sized businesses (SMBs) are particularly susceptible to cyber-attacks. Because they are easier targets than larger companies with more sophisticated security measures, small and medium-sized businesses (SMBs) are frequently the target of cybercriminals (Amrin, 2014).

Despite the fact that most small and medium-sized businesses (SMBs) in developed nations like the United Kingdom, Canada, and the Netherlands use firewalls and antivirus software that is up to date, it appears that these companies are unprepared to handle a sizable number of cyber security incidents. In point of fact, only 13% of small firms and 36% of medium-sized businesses in the United Kingdom train their employees on cyber security. Furthermore, only 19% and 42% of these businesses have reviewed their response to hypothetical situations (Johns 2020, 2021). Less than half of the Canadian companies that have reported using Internet of Things devices have examined the level of security they offer (Statistics Canada 2020).

The consequences of cybercrime against small and medium-sized businesses (SMBs) may extend beyond the organisation that was specifically targeted. For instance, the private and financial information of customers may be at danger if a cyberattack on a small to medium-

sized business (SMB) compromises customer information. Because of this, consumers can stop believing in and trusting the business, which could be bad for its reputation.

Small and medium-sized businesses (SMBs) must be aware about the best defenses against cyberattacks due to the rising threat that cybercrime poses. However, a deeper understanding of the difficulties that small and medium-sized enterprises face both inside and outside of their organisation is necessary to identify the appropriate security solutions to safeguard them against cyber-attacks (Alahmari & Duncan, 2020). This can be helpful in establishing whether the risk mitigation measures will make use of artificial intelligence (AI), cloud computing, or internal policy control, among other options.

1.1. Research Aims and Objectives

This research aims to present an improvement on how to curtail cyberattacks among the small and medium businesses (SMBs).

The objectives of the proposed study are to:

1. Gain a deeper understanding of the types of threat caused by cybercrime to SMBs.
2. Analyse the factors that lead to cybercrime against SMBs.
3. Propose an emerging technology to provide a more secure digital environment for SMBs.

1.2. Research Questions

RQ1: What are cyber threats affecting SMBs and what is the financial impact?

RQ2: What SMB network assets are most targeted, and what vulnerabilities are they exploiting to gain access?

RQ3: What preventive security measures/mechanisms can be employed to mitigate cyber threats in an SMB?

1.3. Scope Of the Study

According to Word Bank (2023), the vast majority of companies worldwide fall under the category of small and medium-sized businesses (SMBs), which are crucial to the creation of jobs and the growth of economies around the world. They account for around 90% of all businesses and more than 50% of all jobs throughout the world.

Due to the expansion of this industry, this research will only target SMBs which heavily utilise internet access for day-to-day business success. The SMBs which do not include required internet services will be excluded.

1.4. Limitation Of the Study

Due to the research delivery time, this research will only analyse information from 50 respondents which meet the inclusion criteria. The criteria ensures that errors due to biases are highly mitigated.

1.5. Research Structure

In chapter 2 of this research, a critical review of the past work in the same field by other researchers would be presented. In addition to this, the conceptual framework of this study will

be established, and the relevant literature gap will be uncovered. Documentation of the research methodology will be presented in Chapter 3. This chapter will provide detailed documentation of the data collection as well as the data analysis. In chapter 4, the analytical report of the analysed data will be discussed. In Chapter 5, the author will analyse the planned study and compare it to previous studies that have been done in the same or a related domain; the novelty of the project depends on this comparison. The research result and recommendations will be presented and discussed in chapter 6 (fig 1.1).

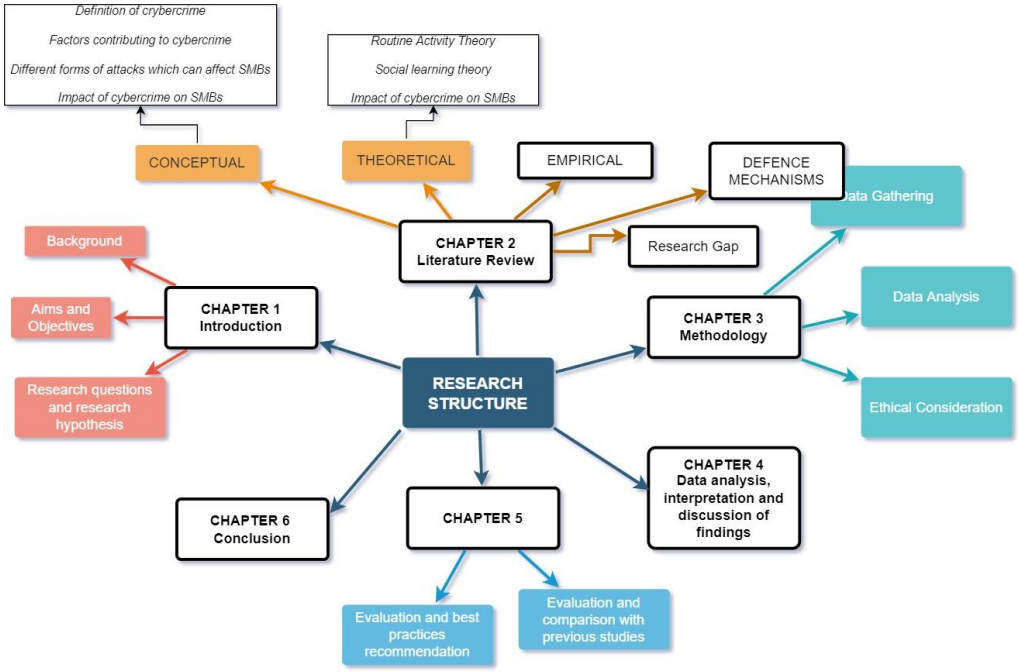

Figure 1 Research Structure

1.6. Definition of Technical Terms

Small and Medium Businesses (SMBs): Companies that fall below a specific benchmark in terms of their revenues, assets, or workers number are referred to as "Small and Medium businesses." The SMBs are defined differently in each country. E.g., In the United Kingdom, Small Business: typically defined as a business with fewer than 50 employees while Medium-Sized Business: Generally defined as a business with fewer than 250 employees.

Cyberattacks: A cyberattack is any offensive maneuver aimed at computer information systems, computer networks, infrastructure, or personal computer devices.

2. Literature Review

This chapter will document the previous research works on different cyberattacks on SMB. This will start with the conceptual review, followed by the theoretical review then lastly by the empirical review. This chapter will identify the common defensive mechanism available in an organisation and how SMBs are improving their cyber security defense, necessary gaps of literature as identified from the critically analysed papers. Then sealed by the general conclusion.

2.1 The Conceptual Review

Businesses of all sizes are becoming increasingly concerned about cybercrime, but SMBs are particularly vulnerable to its disastrous effects (Frank et.al, 2022). Such businesses might not have the same level of cybersecurity expertise as larger companies because they sometimes have limited resources (Amrin, 2014). In this conceptual overview, the causes of cybercrime and how it affects SMBs will be examined.

This conceptual review is crucial because it establishes the groundwork for comprehending the specific difficulties SMBs confront in connection to cybercrime (Paoli et al., 2018). This will help to find out more about the specific threats faced by SMBs by examining the elements that contribute to cybercrime, such as technology weaknesses, social engineering techniques, and insufficient cybersecurity measures. To effectively reduce cyber threats and safeguard SMBs from potential harm, it is essential to understand these aspects (Paoli et al., 2018). Furthermore, by focusing on how cybercrime affects SMBs, we can highlight the negative effects in terms of monetary losses, reputational harm, and operational interruptions. This information may help in increasing awareness of the urgent need for better cybersecurity measures and support among SMBs and policymakers (Alahmari & Duncan, 2020).

2.1.1 Definition of Cybercrime

Cybercrime is a criminal activity that is committed using a computer or the internet. It can take many forms, including hacking, phishing, identity theft, and malware attacks. Cybercriminals target both individuals and organizations, with the goal of stealing personal or sensitive information, extorting money, or causing damage to computer systems.

2.1.2 Factors Contributing to Cybercrime

To understand the best step against cyberattacks, it is a good step to know the factors contributing to this cybercrime (Abel & Francisca, 2023; Lee & Wang, 2022). There are several factors that contribute to the prevalence of cybercrime which include:

Technology Advances - Advances in technology have made it easier for cybercriminals to target SMBs. For instance, cloud computing and the Internet of Things (IoT) have created new attack vectors that can be exploited by hackers.

Insufficient Cybersecurity Measures - Many SMBs do not have the necessary resources or expertise to implement effective cybersecurity measures. This can include outdated software, lack of employee training, and weak passwords.

Lack of Awareness - Some SMBs may not be aware of the risks associated with cybercrime or may not take the threat seriously. This can lead to a lack of preparation and inadequate protection against cyberattacks.

Increased Remote Workforce - With the rise of remote work, many SMBs have had to adapt quickly and may not have the necessary security measures in place to protect their networks and data.

2.1.3 Different Forms of Attacks which can Affect SMBs

There are several forms of cyberattacks that can affect SMBs, each with its own characteristics and potential impact. The need to understand the target by cyber-attackers to help mitigate their attempts in a SMBs is also important. Fig 2.1 shows that most of the vulnerable industries are the manufacturing industries.

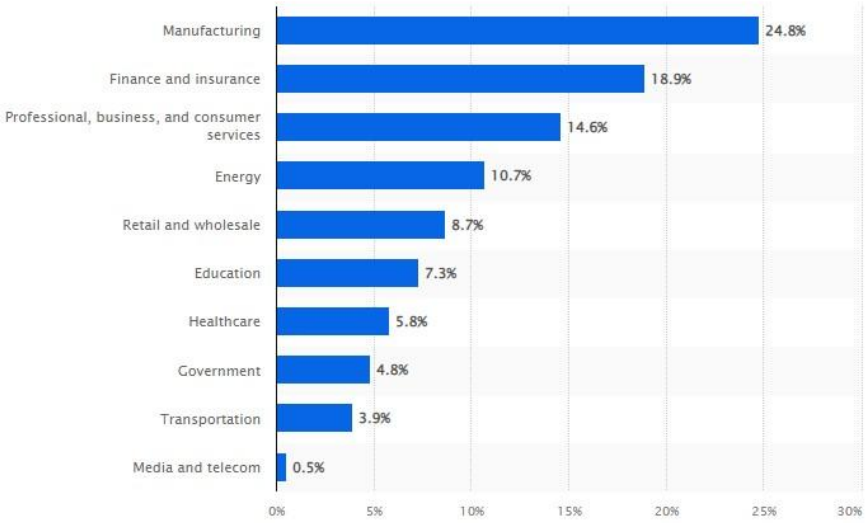

Figure 2.1 Share of cyberattacks among industries.

Malware attacks: Malware is a type of malicious software that can be installed on a computer system without the user's knowledge or consent. Malware attacks can take various forms, including viruses, trojans, ransomware, and spyware. According to figure 2.2, the level of malware attacks of the past 3 years seems to be on similar range which is lower than the experience around the year 2018-2019. The major rise in the malware attack in the year 2018-2019 can be attributed to the emergence of cyber match. As many businesses see the online platform as the medium to maintain their services due to the effect of Covid-19 (fig 2.2).

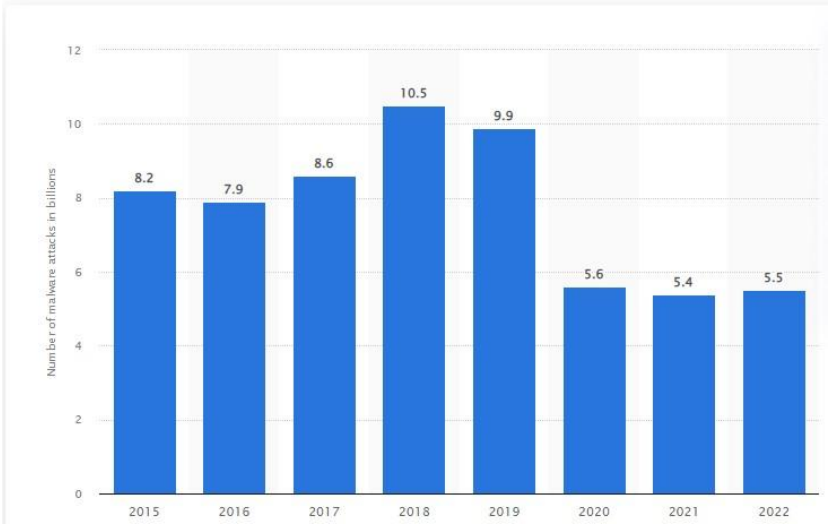

Figure 2.2 Number of malware attacks over the past 8 years

Phishing attacks: Phishing is a social engineering technique that involves sending fake emails or messages to trick users into revealing their personal or financial information. Phishing attacks can be highly effective, as they often appear to come from legitimate sources and use persuasive language and urgent requests to persuade the user to click on a link or enter their login credentials. According to figure 2.3, 27% of the organisations experience successful phishing attacks globally in the year 2021.

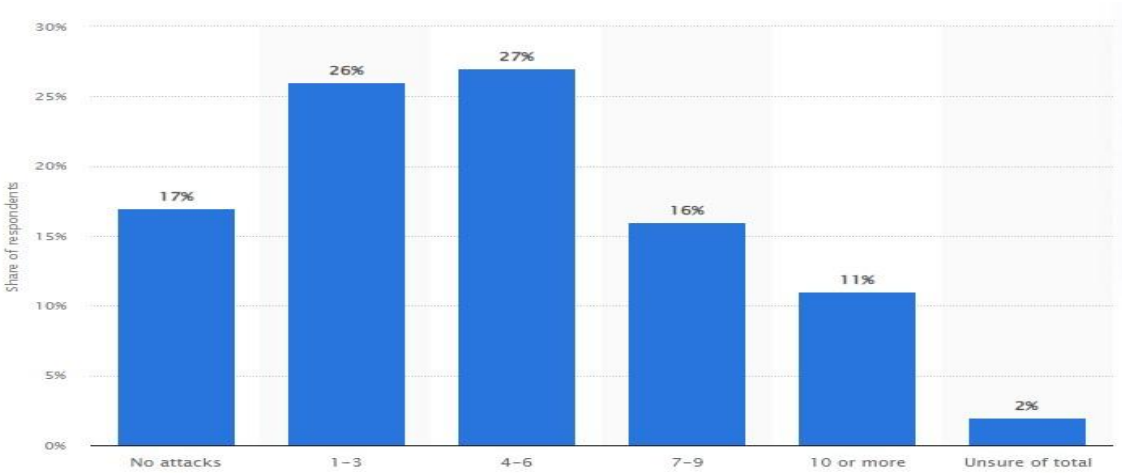

Figure 2.3 Share of phishing attacks among organisations globally.

Figure 2.3 shows that 26% and 27% of the organisations confirm that they experienced 1-3 and 4-6 cyberattacks respectively. Whereas only 2% of the organisations are unsure of the total phishing attacks experience. The increase in phishing attacks vulnerabilities shows the need for improvement that can help drastically reduce this risk.

DDoS attacks: A Distributed Denial-of-Service (DDoS) attack is a type of cyberattack that aims to disrupt the normal functioning of a website or online service by overwhelming it with traffic. DDoS attacks can be launched from multiple sources and can be difficult to mitigate, leading to prolonged downtime and lost business.

The research by Bender (2018) claimed that as part of the annual study performed by Kaspersky Lab, in April 2017 shows that over 5,200 decision-makers from small, medium, and large companies in 29 countries were asked questions about security issues and cyber security incidents. From the result of their findings, it was proven that the costs of DDoS attacks are increasing significantly (Bender, 2018). The cost that can be lost due to DDoS among SMBs were projected to be 123,000 US dollars per attack. However, in the case of large companies, a DDoS attack was projected to hit with financial damage of 2.3 million dollars on average (Bender, 2018).

However, the level of attacks by countries shows that the IT giants such as US, UK, China leads the most vulnerable countries facing the DDoS attacks (fig 2.4).

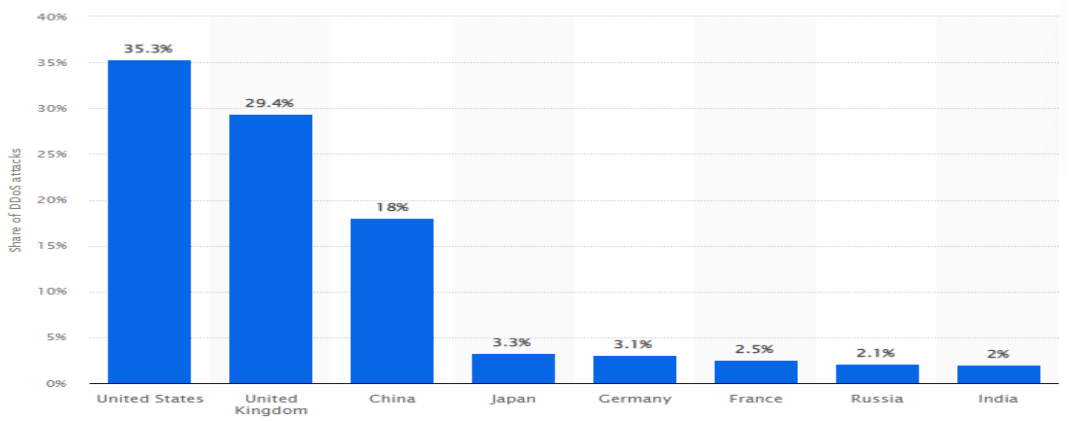

Figure 2. 4 Share of DDoS attacks per country

Man-in-the-middle attacks: A Man-in-the-Middle (MITM) attack involves intercepting communications between two parties and altering the messages to gain access to sensitive information. This type of attack can be particularly devastating for SMBs, as it can compromise their entire network infrastructure and result in significant financial losses.

Taylor (2023) claims that MITM attacks are rather prevalent, typically occurring on a small scale. According to Taylor (2023), around 35% of attacks that target cyber weaknesses are MITM attacks. Hackers can log onto a Wi-Fi network in a cafe or airport and quickly achieve their goal without any traces (Taylor, 2023).

SQL injection attacks: A SQL injection attack is a type of cyberattack that targets the databases of a website or web application. By injecting malicious code into the SQL query, attackers can gain access to sensitive information, such as customer data and financial records. SQL injection attacks can also be used to insert or delete data, leading to significant data loss and system downtime. The SQL injection is one of the most popular cyber-threats in web applications (Fig 2.5).

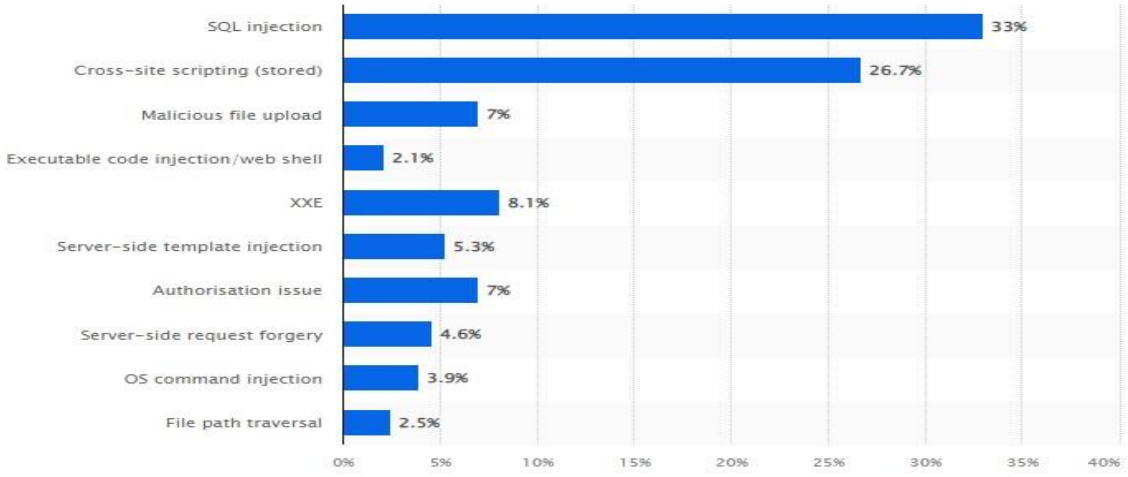

Figure 2.5 Share of web vulnerabilities.

Insider threats: Insider threats involve attacks from within an organization, such as employees or contractors who have access to sensitive information or systems. Insider threats can take various forms, including theft of data, sabotage of systems, or installation of malware (Saxena et.al, 2020). SMBs are particularly vulnerable to insider threats, as they often have limited resources for monitoring and controlling access to sensitive information (Saxena et.al, 2020).

According to Verizon (2019), insider threats are one of the most frustrating cyberattacks. The report shows that 57% of the databases which were breached were due to an insider attack, similarly, 20% of cyber security incidents and 15% of data breaches are due to misuse of privilege, which can be caused by an insider attack (Verizon, 2019).

This cyberattack is a growing issue that can place employees and customers at risk and cause financial harm to a business. As more employees gain access to multiple accounts containing more data, internal threats within small businesses increase. According to research conducted by Sylvester (2018), 62% of employees have reported having access to accounts that they presumably do not need. As reported by Tessian (2022), almost all the industries are facing

insider threat attacks, and the initial step which is downloading the resources of the companies into a personal computer is common among all (fig 2.6).

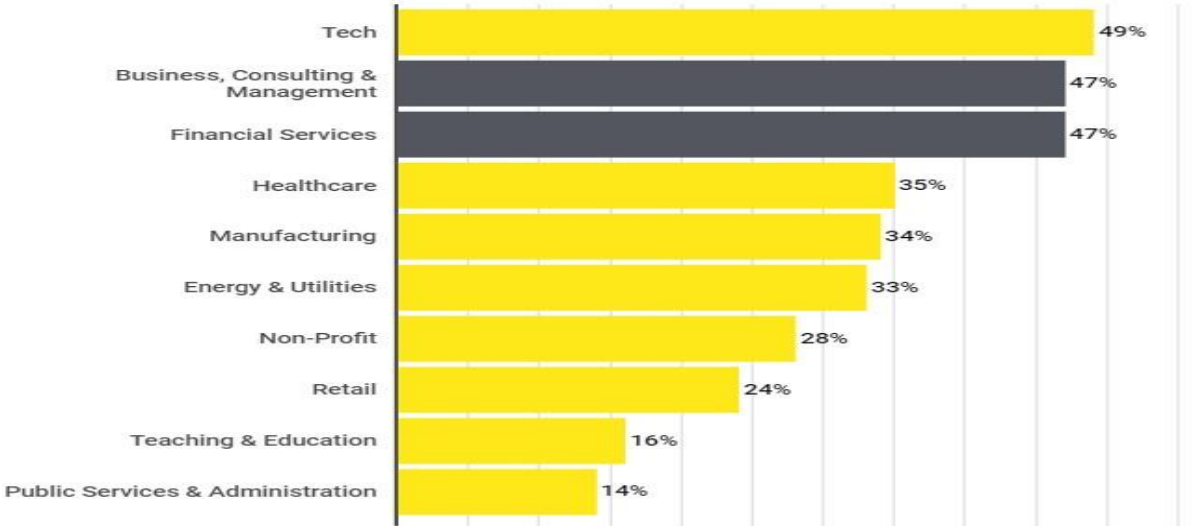

Figure 2.6 Percentage of employees downloading company resources into the personal PC (Tessian, 2018)

Ransomware attacks: Ransomware is a type of malware that encrypts the victim's files and demands payment in exchange for the decryption key. Ransomware attacks can be devastating for SMBs, as they can result in significant financial losses, lost productivity, and reputational damage.

In the last two quarters of 2022, global ransomware attacks increased by over 50 %, from over 102 million to nearly 155 million cases, according to Ani (2023). The maximum number of global ransomware attacks was recorded in the second quarter of 2021, when 188.9 ransomware attacks were reported by organisations worldwide (Fig 2.7).

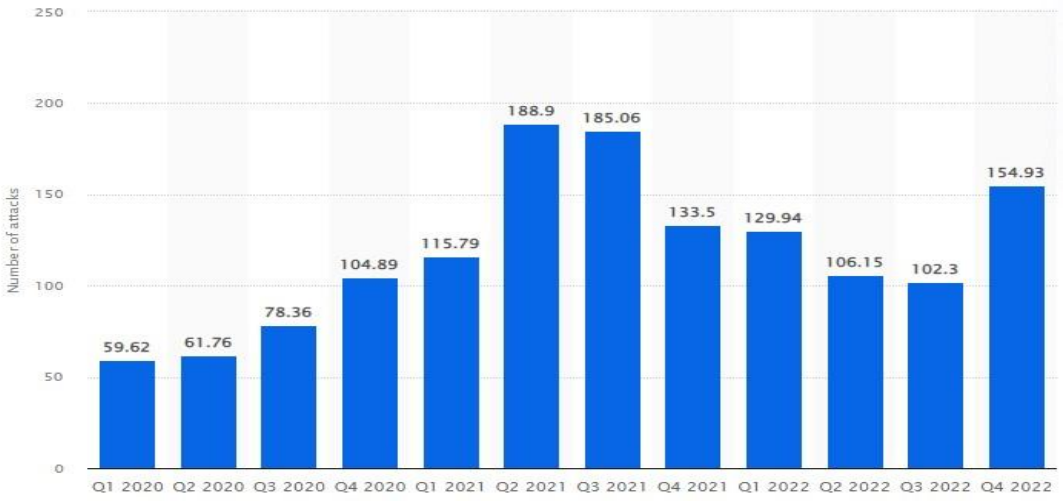

Figure 2.7 Number of Ransomware attacks (Statista, 2023)

Supply chain attacks: Supply chain attacks involve targeting the third-party vendors and suppliers of an organization to gain access to their systems or data. SMBs are particularly vulnerable to supply chain attacks, as they often rely on a limited number of vendors and may

not have the resources to conduct thorough due diligence on their cybersecurity practices. The report by Lionel (2023), shows that this type of attack is increasing yearly (Fig 2.8).

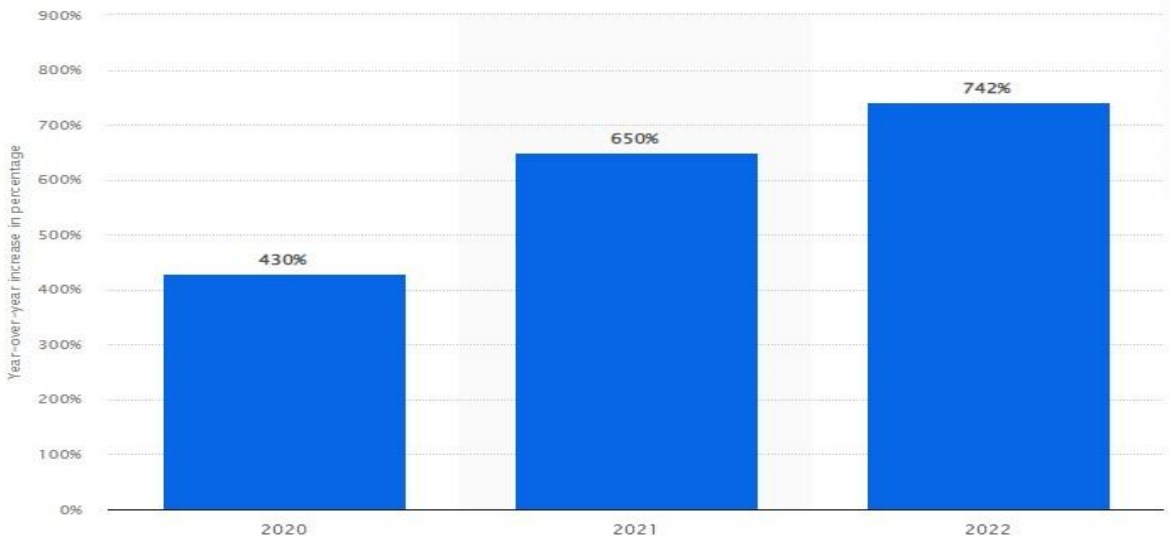

Figure 2.8 Year over Year (YoY) increase in Supply chain attacks (Lionel, 2023)

2.1.4 Impact of Cybercrime on SMBs

The impact of cybercrime on SMBs can be significant and wide-ranging (Lee & Wang, 2022). These impacts can be classified into direct and indirect impacts.

Direct impacts include financial losses, damage to reputation, and legal and regulatory consequences. Financial losses can result from stolen funds or the cost of repairing damaged systems. Damage to reputation can occur when an SMB's customers lose trust in the business due to a cyberattack. Legal and regulatory consequences can include fines and lawsuits. Indirect impacts include lost productivity and lost business opportunities. Cybercrime can cause disruptions in business operations, leading to lost productivity. It can also lead to lost business opportunities when customers choose to do business with competitors that they perceive to be more secure.

According to Lee & Wang (2022), the impact of cybercrime on Small and Medium-sized Businesses (SMBs) can be significant and wide-ranging, depending on the level of the attack. Key impacts include financial loss, which can be direct, such as stolen funds or the cost of repairing damaged systems, or indirect, like lost productivity and business opportunities. Cybercrime can also damage an SMB's reputation, eroding customer trust and potentially having long-term consequences, especially for businesses that rely on their reputation to attract and retain customers. Legal and regulatory consequences, such as fines and lawsuits, can also result from cybercrime, posing a particular challenge for SMBs that may lack the resources to handle these consequences. Lastly, the psychological impact of cybercrime on SMB owners and employees, including stress, anxiety, and a sense of violation, should not be overlooked.

2.3 The Empirical Review

In this section, empirical studies will be conducted to investigate the factors and impact of cybercrime on SMBs. These studies will shed light on the nature of cybercrime incidents, the vulnerabilities of SMBs, and the effectiveness of different cybersecurity strategies from other

researchers' perspectives. The empirical review is of great importance as it provides real-world evidence and insights into the factors and impact of cybercrime on SMBs. By examining empirical studies, we can gather quantitative and qualitative data on cybercrime incidents experienced by SMBs, the specific attack vectors used, and the resulting consequences (Noche, 2021). These studies can help identify patterns, trends, and commonalities among cybercrime incidents, enabling us to better understand the modus operandi of cybercriminals targeting SMBs.

Moreover, empirical studies can highlight the vulnerabilities that make SMBs attractive targets for cybercriminals. These vulnerabilities may include inadequate employee training, outdated software, insufficient security protocols, or a lack of dedicated cybersecurity personnel. Understanding these vulnerabilities is crucial for devising targeted interventions and recommendations to strengthen the cybersecurity posture of SMBs. Additionally, empirical studies can evaluate the effectiveness of various cybersecurity strategies employed by SMBs in mitigating cyber threats. By examining the outcomes of different approaches, such as network monitoring, incident response plans, employee awareness programs, or encryption technologies, we can identify best practices and lessons learned (Kergroach et al., 2022). This knowledge can inform SMBs about the most effective strategies to adopt and guide policymakers in designing supportive frameworks for SMB cybersecurity.

The research conducted by Symantec (2016) shows that in 2015, 43% of cyberattacks targeted small and medium-sized businesses (SMBs). The research also discovered that SMBs are frequently targeted by cybercriminals because of their constrained resources and ignorance of cybersecurity, making them an easier target. According to the research, ransomware, malware, and phishing attacks are the most typical forms of cyberattacks against SMBs (Symantec, 2016).

The report of IBM (2019) shows that the average cost of a cyberattack for SMBs in 2019 was $2.2 million. The report also discovered that malicious insider cyberattacks on SMBs were the most expensive, with an average cost of $243,000 per incident. The report emphasised how crucial it is to have a cybersecurity plan in place in order to lessen the effects of cyberattacks (IBM, 2019).

According to the National Cyber Security Alliance (NCSA, 2019), 60% of SMBs fail within six months following a cyberattack. The report also discovered that DDoS attacks, ransomware attacks, and phishing attacks are the most typical forms of cyberattacks against SMBs. The research emphasised how crucial it is for SMBs to take preventative measures against cyberattacks by putting in place strong security measures, holding routine cybersecurity training sessions, and creating an incident response strategy.

SMBs are particularly susceptible to cyberattacks because of their scarce resources and lack of cybersecurity expertise, according to a University of Maryland study (University of Maryland, 2019). According to the research, phishing, malware, and ransomware attacks are the most frequent types of cyberattacks on SMBs. The report emphasised how crucial it is for SMBs to take proactive actions to safeguard their systems and data, like deploying anti-malware software, creating secure passwords, and performing regular backups.

According to a research by Verizon (2019), 43% of cyberattacks target small and medium-sized businesses, and 60% of those businesses fail within six months of a cyberattack (Verizon,

2019). The report also discovered that ransomware, malware, and phishing attacks are the most frequent types of cyberattacks against SMBs. The report emphasised how crucial it is for SMBs to put strong security measures in place to safeguard their systems and data, including two-factor authentication and encryption.

Small and medium-sized businesses (SMBs) need to pay greater attention to cybersecurity risks because management frequently undervalues them, this is one of the important point from the research by Alahmari & Duncan (2020).

More empirical research is required in the expanding field of cybersecurity risk management in SMBs. The researchers also stressed that SMBs should prioritise cybersecurity because the use of IT technology, such as cloud computing, might make an organisation a high-priority target for hackers (Alahmari & Duncan, 2020).

The research by Frank et.al (2022) indicated that the absence of data on cyber risk poses a severe problem for stakeholders trying to address the cyberattack issues, including academics, insurers, and policymakers. This is because data specificity is essential for better AI model development, risk assessment, pricing for cyber insurance, and evaluating internal cyber posture and cybersecurity actions. Frank et al. (2022) made an effort to give a thorough analysis of the open datasets that were accessible, facilitating timely and effective advancement in cyber risk research and enhancing the dynamic character of cyber-threats.

In order to protect an organization's ICT environment and data from cyber threats, cybersecurity policies are crucial, according to research by Mishra et al. (2022). In the paper, 10 common cybersecurity policy aspects are identified, including privacy, website, cloud computing, email, physical, network, information, access control, data retention, and data protection. The paper compares the cybersecurity policies of various industries, including healthcare, finance, aviation, education, and e-commerce. The study emphasises the significance of selecting the most pertinent cybersecurity policies based on the circumstances of a particular organisation (Mishra et al., 2022).

According to the study, the type of information under control and the security requirements of organisations in connection to these policies impact the choice and applicability of cybersecurity policies (Mishra et al., 2022).

In conclusion, it can be pointed out that the empirical research has revealed that cybercriminals are increasingly focusing on SMBs, with phishing, malware, and ransomware attacks being the most frequent types of cyberattacks. These have also emphasised SMBs' weaknesses, such as their constrained funding and lack of cybersecurity expertise, and the significance of SMBs taking preventative actions to protect their systems and data. These steps entail putting in place strong security safeguards, completing routine cybersecurity training, and creating an incident response strategy. SMBs can lower their cybersecurity risks and lessen the effects of cyberattacks by following these measures.

2.4 Defensive Mechanisms for Cyber Attacks

According to a study by Pedreira et al. (2021), the defense mechanisms commonly used by SMBs against cyber-attacks were categorized into six groups: Application, Devices, Network, Social Engineering, Policy, and Physical Security. However, the effectiveness of these mechanisms varies depending on the type and severity of the attack. SMBs' owners seem to be

lagging behind in terms of investing on the security of their organization (Fig 2.9). To improve their cybersecurity, SMBs should consider implementing effective co-operation mechanisms and good channels of communication to identify and respond to emerging threats (Kergroach et al., 2022). In addition, some general measures that SMBs can take to protect themselves from cyber threats include backing up their data, securing their devices and network, encrypting important information, and ensuring that their software is up to date (Australian Government, 2021).

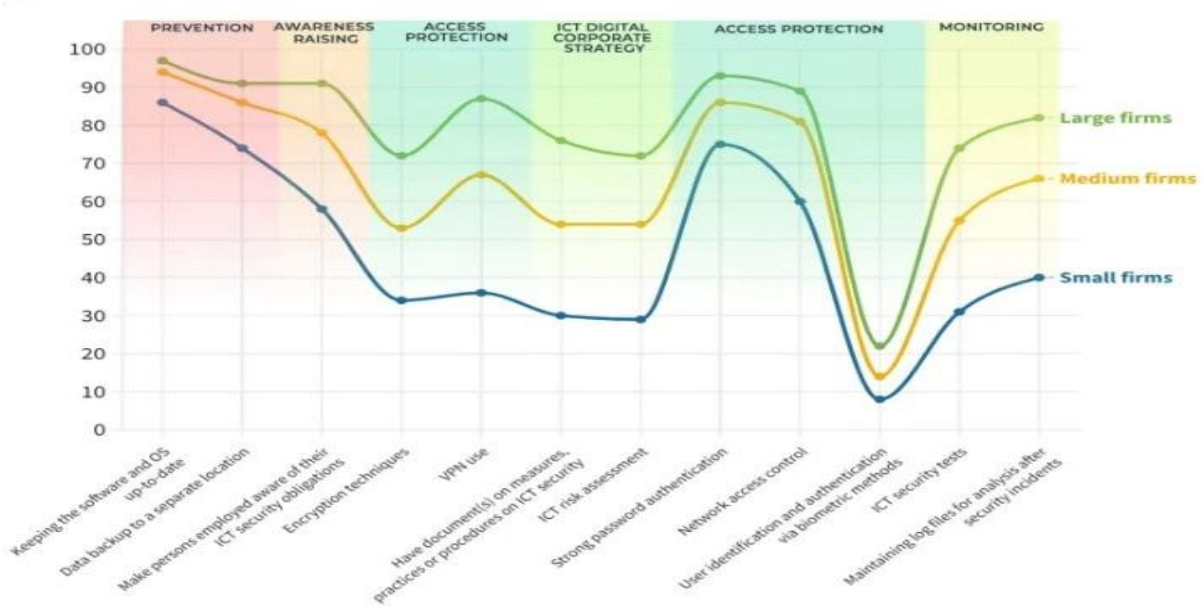

Figure 2.9 Percentage of enterprises implementing ICT digital security measures, by type of measures and firm size.

2.5 Gap of Literature

While there has been considerable research on cybercrime and its impact on SMBs, certain gaps in the existing literature remain. Identifying these gaps is crucial for directing future research efforts and enhancing our understanding of the complex dynamics surrounding cyber-attacks against SMBs.

One significant gap is the limited focus on the specific challenges faced by different industries within the SMB sector. Cyber threats and vulnerabilities can vary depending on the nature of the business, its sector, and the type of data it handles. Further research is needed to explore sector-specific cyber threats, develop tailored defensive strategies, and assess the effectiveness of industry-specific cybersecurity measures.

Another gap in the literature lies in the evaluation of emerging technologies and their potential for enhancing SMB cybersecurity. As cyber threats continue to evolve, exploring the effectiveness of technologies such as artificial intelligence, machine learning, and behavioral analytics tools like Datadog, Splunk, Grafana Labs, etc. becomes crucial, however, the cost of these tools are also very important for an SMBs. Understanding how these technologies can be leveraged by SMBs to detect, prevent, and respond to cyber-attacks is an area ripe for exploration.

Furthermore, literature would benefit from more studies that investigate the human factor in cyberattacks against SMBs. While technical defenses are essential, it is important to recognize the role of human behavior in cybersecurity incidents. Exploring the influence of employee training, organizational culture, and user awareness on mitigating cyber risks can provide valuable insights for developing holistic defensive mechanisms.

Additionally, there is a need for more empirical studies that analyze the financial impact of cyber-attacks on SMBs. Understanding the economic consequences, such as financial losses, recovery costs, and long-term business viability, can help SMBs and policymakers prioritize cybersecurity investments and allocate resources effectively.

Due to the limited time, this research will contribute by proposing a framework which can guide SMBs on how to integrate AI and the behavioral analytical tool in their service to defend their assets against cyber-attacks.

2.6 Conclusion

A variety of causes, such as technical development, insufficient cybersecurity safeguards, a lack of knowledge, and an increase in remote employment, have contributed to the rise in cybercrime. As documented in this research, SMBs may suffer financial losses, reputational damage, legal and regulatory implications, and psychological problems as a result of cybercrime. Although cybercrime still poses a serious danger to SMBs, theoretical frameworks and cybersecurity models offer helpful direction for comprehending the causes of cybercrime and its effects on SMBs. SMBs must therefore properly consider the threat posed by cybercrime and take precautions to safeguard their networks and data. This entails putting in place reliable cybersecurity safeguards, training staff members, and keeping abreast of the most recent cybercrime risks and trends. Emerging technologies like AI and cloud computing offer SMBs promising ways to strengthen their cybersecurity and defend against cyberattacks. To execute successful cybersecurity measures, it is necessary for SMBs to prioritise cybersecurity, in addition to adopting the necessary technologies.

3. Practical Research Methodology

The present section covers various aspects of research methodology, including research design, data collection, population, instrument validity, sampling and reliability, variable measurement, and analytical procedures.

3.1 Research Design

This study utilises a quantitative research design to investigate the factors contributing to cybercrime against small and medium-sized businesses (SMBs). Critical design of research methodology is important to propose emerging technologies which the SMBs can use to mitigate the cyber threat (Moeuf et.al, 2019). A survey-based approach will be employed, utilizing a structured questionnaire to collect data from participants. The questionnaire will be designed to gather information related to cyber threats, financial impact, targeted network assets, vulnerabilities, and preventive security measures in SMBs.

3.2 Sample Selection

The target population for this research includes small and medium-sized businesses that heavily rely on internet access for their day-to-day operations. A purposive sampling technique will be

employed to select the sample for the study. The sample will consist of SMB owners, managers, and IT personnel who possess knowledge and experience in the use of the internet and cyber security domain. The size of the sample will be determined based on the principle of saturation, aiming to include a sufficient number of participants to obtain comprehensive and meaningful data (Hennink & Kaiser, 2022).

3.2.1 Sample Size and Sampling Techniques

To ensure a diverse representation, the sample will include businesses from different numbers of employees and industries. The justification for selecting a sample size of 400 respondents is based on the principle of saturation (Hennink & Kaiser, 2022; Alvi, 2016). This principle suggests that data collection should continue until the point of redundancy, where new data no longer provide substantially different insights or contribute to the research objectives (Hennink & Kaiser, 2022). By including 400 respondents, we aim to reach a level of data saturation where the collected information is diverse and comprehensive enough to address the research questions effectively.

3.3 Data Collection Procedure

Data will be collected through a self-administered online questionnaire developed through Qualtrics. The questionnaire will be designed based on the research objectives and research questions outlined in Chapter 1. It will consist of both closed-ended and Likert-scale questions for enough and easy data collection. The questionnaire will be pilot tested with a small group of participants to assess its clarity, comprehensibility, and reliability this is in accordance with the research conducted by Tojib & Sugianto (2006). Necessary adjustments will be made based on the pilot study results before the final survey is distributed.

3.4 Data Analysis

The collected data will be analyzed using appropriate statistical techniques. Descriptive statistics, such as frequencies, percentages, means, and standard deviations, will be employed to summarize the demographic characteristics of the participants and provide an overview of the research variables (Liang et.al, 2017). Regression analysis may be utilized to determine the factors influencing the occurrence of cyberattacks and to evaluate the effectiveness of preventive security measures. The analysis will be performed using statistical software, such as SPSS and Excel for proper visualization.

3.5 Measurement of Variables

The measurement of variables is a crucial aspect of this research methodology as it ensures the accurate and reliable collection of data through the questionnaire. This section provides an introduction to the measurement process, highlighting the variables considered and the corresponding measurement scales used.

In this study, a total of 15 questions were asked which helps to investigate the factors, impacts and necessary mitigation steps of cybercrime on small-to-medium-sized businesses (SMBs). These research questions can be categorized under the variables which are:

1. Cybercrime incidents: This variable aims to capture the frequency and nature of cybercrime incidents experienced by SMBs. It will be measured using a categorical

scale, allowing respondents to indicate the presence or absence of specific types of cybercrime incidents.

2. Vulnerabilities: The vulnerabilities of SMBs that make them susceptible to cyber-attacks will be assessed. This variable will be measured using a Likert scale, allowing respondents to rate the extent of vulnerabilities they perceive within their organizations.
3. Cybersecurity measures: The effectiveness and adoption of cybersecurity measures within SMBs will be evaluated. This variable will be measured using a combination of categorical and Likert scales, enabling respondents to indicate the presence or absence of specific measures as well as rate their effectiveness.
4. Impact of cybercrime: This variable aims to assess the consequences of cybercrime incidents on SMBs, including financial losses, reputational damage, and operational disruptions. It will be measured using a Likert scale, allowing respondents to rate the severity and impact of these consequences.

The measurement scales selected for each variable have been chosen to capture the nuances and variations within the research aims and objectives while ensuring ease of respondent understanding and efficient data analysis.

3.6 Reliability and Validity of Research Instrument

During the course of this research, both the appearance and the substance of the validity of the instrument that was used were given significant thought. The Qualtrics software used for the development of the questionnaire has been tested and validated. For the questionnaire, my supervisor carefully examined it to ensure that the use of language and he also guided me for the area that needed an improvement before the questionnaire was shared. In addition, he assisted in determining whether the questionnaire items were sufficient to elicit the required data from respondents. After his suggestions for improving the instrument's items were implemented, reliability and validity tests, including the Cronbach Alpha, were conducted to evaluate the performance of the instrument.

3.7 Ethical Considerations

This study has been proposed to the Department of Cybersecurity. The management of the University of Sunderland in the United Kingdom has approved the research. The ethics department has determined whether to grant permission for this research to be conducted using the questionnaire submitted via the Qualtrics form. The researcher's supervisor was asked for permission to undertake the study, which he granted. To safeguard the participants' privacy and anonymity, the study used codes rather than their real names to identify them. Participants who do not comply with the consent form are not obligated to participate. Questionnaires were delivered to the intended respondents using a Qualtrics form. This research's objective and practises are to use the gathered information and data for the indicated purposes. The APA 7 reference style was used, and as a consequence, the work created is unique and free of plagiarism. The research supervisor then approves the study question and subject based on what is judged to be acceptable for investigation.

3.8 Dissertation Project Management Scheduling

Table 3.1 shows the deliverable of this research.

Task	Pre-requisite	Deadline	Deliverable
Introduction	Understanding the research aims and objectives	01/04/2023	Completion of chapter 1
Literature Review	Research topic identification	24/04/2023	Completion of literature review
Research Design	Review of existing research methodologies	20/05/2023	Finalization of research design
Ethics and Compliance	Compliance with ethical and legal requirements	30/05/2023	Ensuring adherence to ethical guidelines and getting approval from the University.
Questionnaire Design	Understanding of SMB cybersecurity challenges	30/05/2023	Completion of questionnaire design
Data Collection	Finalized questionnaire	01/06/2023	Completion of data collection
Data Analysis	Collected data	24/06/2023	Completion of data analysis
Results Interpretation	Analysed data	29/06/2023	Interpretation of research findings
Framework Development	Research findings and analysis	30/06/2023	Development of proposed framework
Evaluation	Proposed framework and feedback from experts	04/07/2023	Completion of framework evaluation
Conclusion and Recommendations	Research findings and proposed framework	10/07/2023	Finalization of conclusions and recommendations
Final Report	Completion of all research tasks and analysis	14/07/2023	Submission of final research report

3.9 Limitations

It is critical to recognise some of this research's shortcomings. First off, because of the unique focus on SMBs that depend heavily on internet connection, the findings' generalizability may be constrained. Without extensive internet usage, the findings might not be applicable to that SMBs.

Due to time constraints, for the research I will only gather responses from a target range of 40-60 respondents. While efforts will be made to ensure representativeness and diversity within this sample, it is important to recognize that a larger sample size may have provided a more comprehensive and generalizable understanding of the factors and impact of cybercrime on SMBs.

Additionally, resource limitations, including access to cyber security organisation which can help to test the effectiveness of the proposed framework may pose challenges in implementing the research proposed framework.

Furthermore, the research's reliance on a questionnaire as the primary data collection method introduces the possibility of response biases and limitations inherent to self-reporting. Despite efforts to ensure clarity and reliability, there is a potential for response biases, such as social desirability bias or recall bias, which may influence the accuracy of the collected data.

Despite these drawbacks, the research seeks to offer insightful analysis of cybercrime directed against SMBs and to suggest practical solutions to the problem.

3.10 Conclusion

The chosen quantitative research design, consisting of a structured questionnaire and statistical analysis permits a systematic examination of the factors that contribute to cybercrime against SMBs. This study aims to acquire a deeper understanding of cyber threats, vulnerabilities, and the impact on SMBs by analysing the collected data. In addition, the study will propose emergent technologies that can improve the security of digital environments for SMBs. Priority will be given to ethical considerations in order to protect participant confidentiality and privacy. Through this research, valuable knowledge can be obtained to assist SMBs in mitigating cyber threats and improving their cybersecurity practices. The following section details the findings of this study.

4. Data Analysis Result & Discussion

The Descriptive Statistics of respondents' demographic data was done, and result shown in table and graphs for clear visualization of insights. Some of the questions in the questionnaire required multiple responses and this prompted the use of Multiple Case Analysis in SPSS. A case summary and data arising from the multiple case analysis on such questions were shown in tables and graphically visualized.

"Multiple Case Analysis" is a methodology that is commonly used in dissertations and research projects to analyse qualitative data. It involves evaluating responses from several participants or cases to uncover similar patterns, themes, and trends in the context of analysing questionnaire data. Researchers can use this strategy to obtain a better grasp of the study issue and generate significant conclusions based on the data collected.

4.0.1 Descriptive Statistics of Demographic Data

Deductions from the descriptive statistics (Table 4.0) indicates that the dataset comprises of respondents who are 18years and above (Figure 4.0) with a large number having Bachelor's and Master's degree (Figure 4.1) with specialization in Information Technology, Finance and Education industries (Figure 4.2) and have majorly worked in Small and Medium Businesses (SMBs) (Figure 4.3) for over a year (Figure 4.5) where accounts of Cyber Attacks have been recorded (Figure 4.6).

Table 4.0 Respondents Demographic Statistics

		Frequency	Percentage %
What is your highest level of education completed?	High School Diploma or Equivalent	2	4.4%
	Associate Degree	2	4.4%
	Bachelor's Degree	16	35.6%
	Master's Degree	24	53.3%
	Doctorate Degree	1	2.2%

Which industry does your organization belong to?	Information Technology	23	51.1%
	Finance	8	17.8%
	Healthcare	1	2.2%
	Retail	2	4.4%
	Manufacturing	3	6.7%
	Education	8	17.8%
	Others (Please specify)	0	0.0%
What is the size or your organization?	Small (11 to 50 employees)	15	33.3%
	Medium (51 to 250 employees)	30	66.7%
What is your current role?	IT Support/Analyst	22	50.0%
	Cybersecurity Analyst/Engineer	7	15.9%
	IT Specialist/Consultant	6	13.6%
	Information Security Administrator	2	4.5%
	ICT Administrator	3	6.8%
	Other (Please specify)	4	9.1%
How long have you worked in your current role?	Less than 1 year	12	26.7%
	1-3 years	12	26.7%
	3-5 years	16	35.6%
	5-10 years	4	8.9%
	More than 10 years	1	2.2%
Has your organization ever experienced a cyber-threat or attack?	No	31	79.5%
	Yes (Please provide more details)	8	20.5%

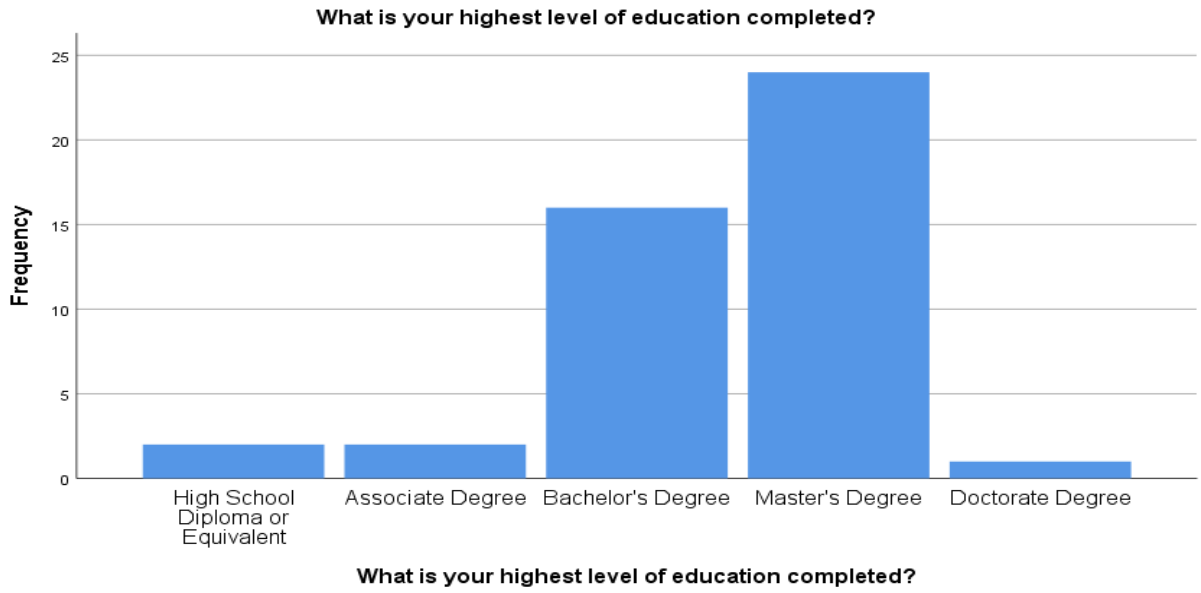

Figure 4- 1 Graph of Level of Education

The educational qualifications of most respondents are mostly bachelor's and master's degree as seen in Figure 4.1.

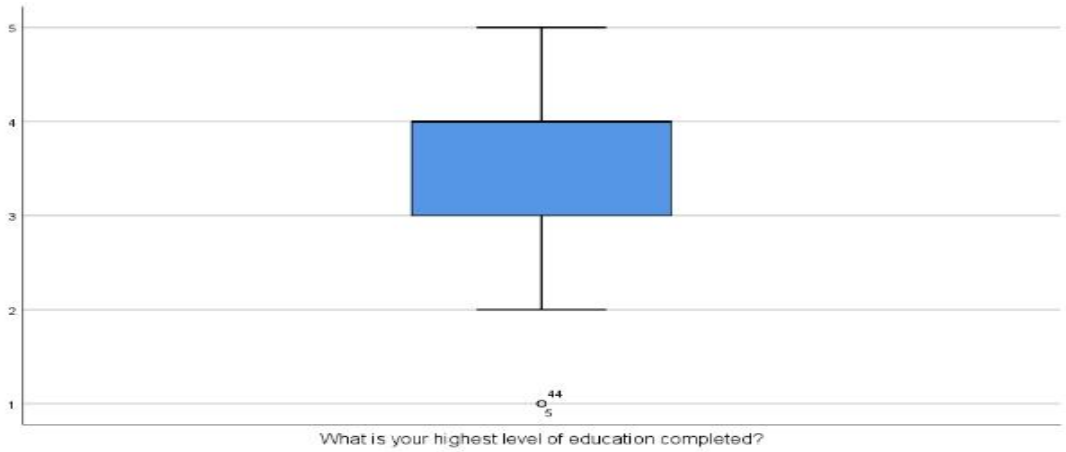

Figure 4- 1B Boxplot of Level of Education

From Figure 4.1B, Outliers are seen in cases 5 and 44 of the dataset and so removed from the analysis.

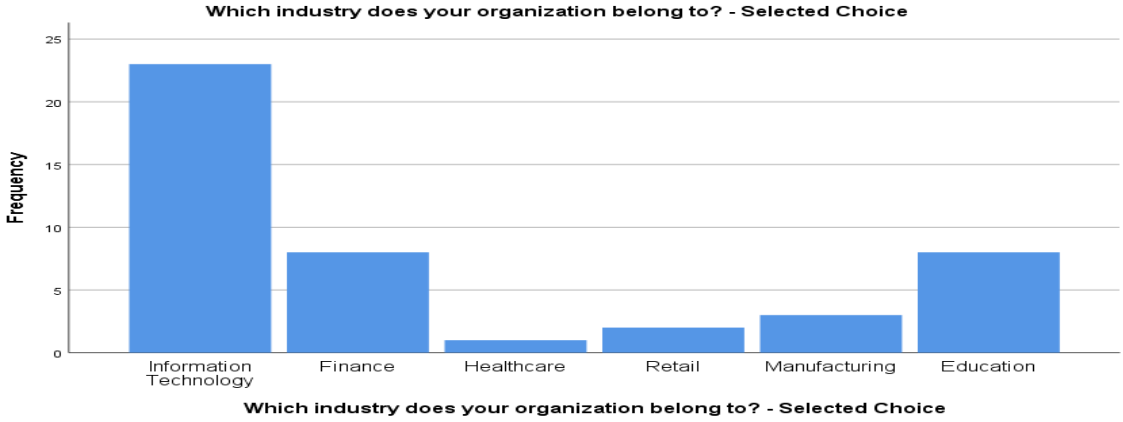

Figure 4- 2 Graph showing respondents' organization.

A very large portion of the respondents are from Information technology organizations as seen in Figure 4.2.

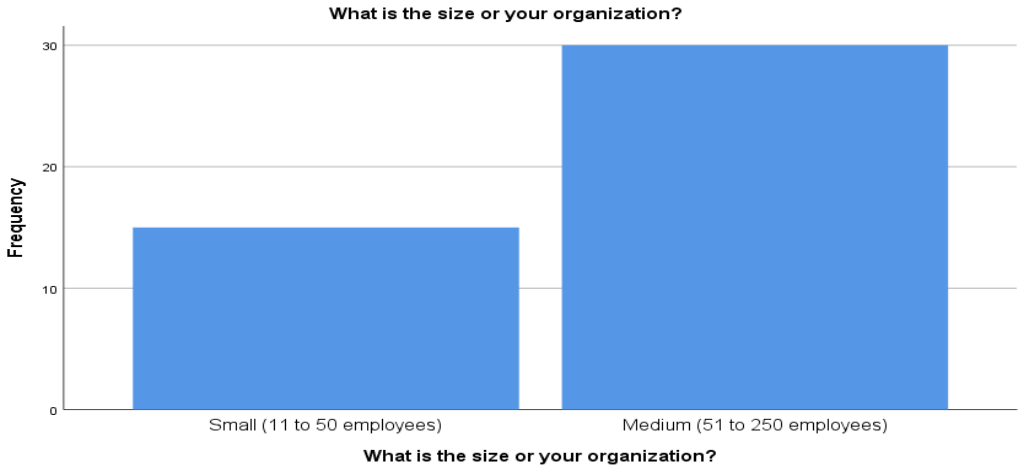

Figure 4- 3 Graph showing Respondents' organization size.

Figure 4.3 shows respondents from medium size organizations participated in the survey.

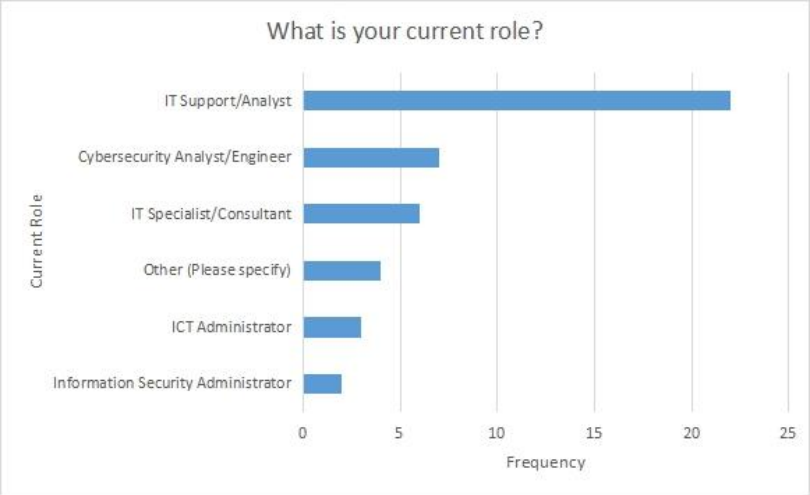

Figure 4- 4 Graph showing respondents' role.

Figure 4.4 shows respondents with IT support/Analyst role amount to 22 in number, which is the highest number recorded.

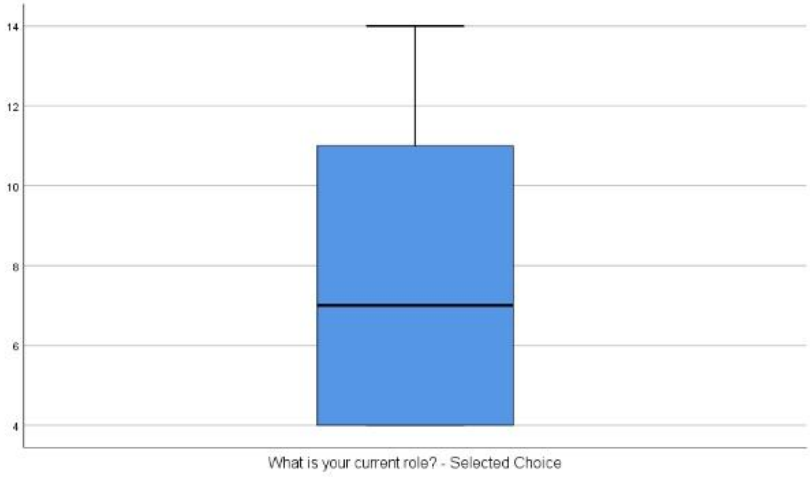

Figure 4- 4B Boxplot of current role

No outliers noticed from Figure 4.4B.

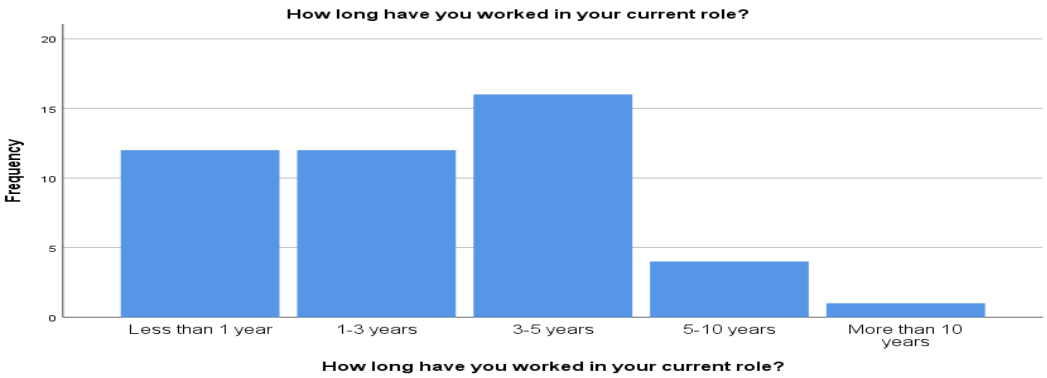

Figure 4-5 Graph showing Respondents number of work years in current role.

From Figure 4.5, 16 of the respondents have worked between 3-5years in their various organizations and this is followed by respondents who have worked for less than 1year and between 1-3years.

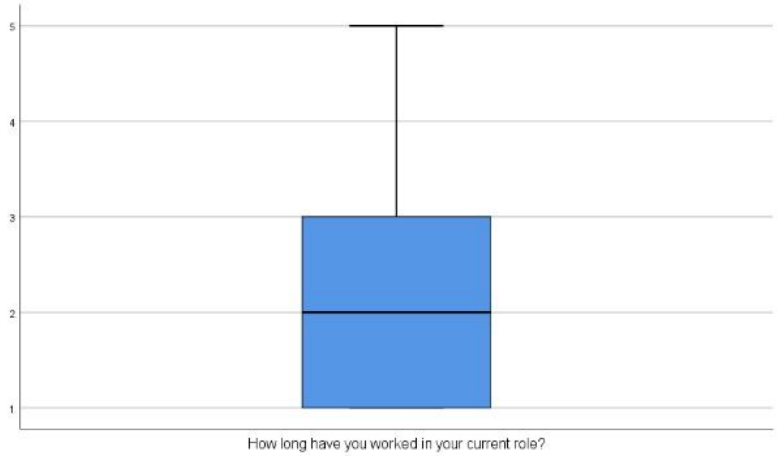

Figure 4- 5B Boxplot of years of service in current role

No outliers noticed from Figure 4.5B.

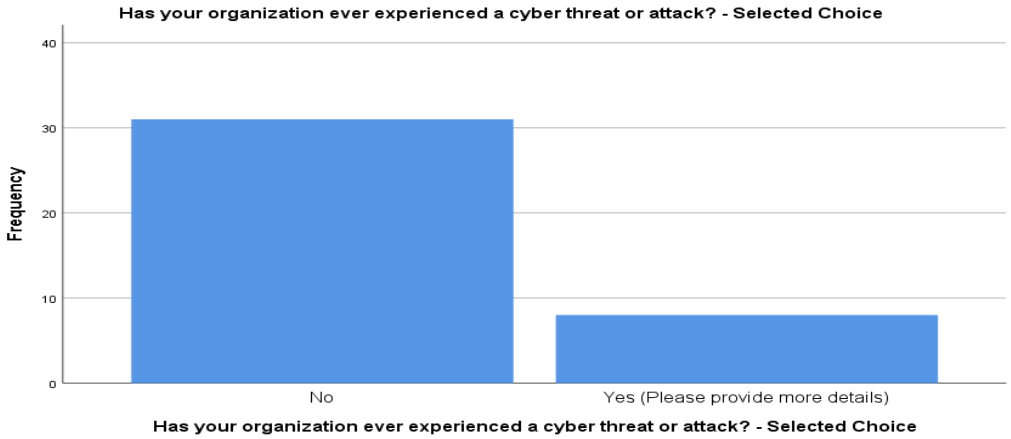

Figure 4- 6 Graph showing information about organization Cyber-threat attacks confirmation.

Though the majority of respondent's organizations have not experienced Cyber-Attacks but a significant number of them have had this unsavory encounter as seen in Figure 4.6.

4.1 Significant Cyber Threats facing SMBs today?

Table 4.1: Case Summary of significant Cyber threat facing SMBs.

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Significant cyber threats facing SMBs today?	39	84.8%	7	15.2%	46	100.0%
a. Dichotomy group tabulated at value 1.						

From Table 4.1, only 39 out of 46 cases are valid which is about 85% of the overall cases, 15 .2% of the cases are missing but considered insignificant and so ignored.

Table: 4.2: Multiple response analysis result of significant Cyberthreat facing SMBs

		Responses		Percent of Cases
		N	Percent	
In your opinion, what are the most significant cyber threats facing SMBs today?	Phishing Attacks	33	33.0%	84.6%
	Ransomware	10	10.0%	25.6%
	Malware	9	9.0%	23.1%
	Distributed Denial-of-Service (DDoS) Attacks	15	15.0%	38.5%
	Insider Threats	17	17.0%	43.6%
	Social Engineering	16	16.0%	41.0%
Total		100	100.0%	256.4%

NOTE: From Table 4.2, the percentage of cases have a total of 256% which is above 100%, this is because each case can have multiple responses, this is clearly seen from the total number of responses of 100 greater than the total number of Cases which is 39.

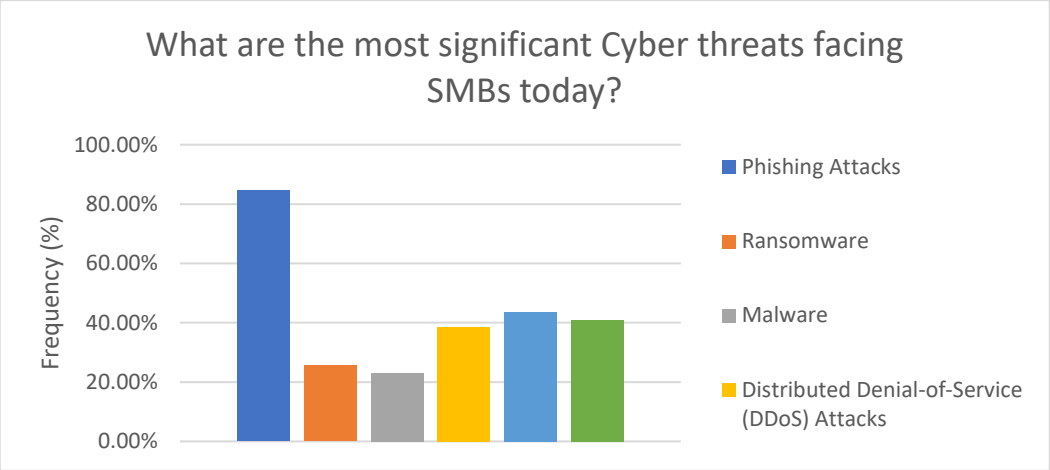

Figure 4- 7 Graph of Significant Cyber threat facing SMBs today.

Graph 4.7 arising from data in Table 4.2 shows Phishing attacks with about 85% as the most significant cyber-threat faced by SMBs, this is followed by Insider Threats with 43.6%. Malware and Ransomware have the least percentage of significance.

4.2 Network assets within SMBs targeted by Cybercriminals.

Table 4.3: Case Summary of Network asset within SMBs targeted by Cybercriminals.

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Network assets within SMBs targeted by Cybercriminals	39	84.8%	7	15.2%	46	100.0%
a. Dichotomy group tabulated at value 1.						

Table 4.4: Multiple response analysis result of Network asset within SMBs targeted by Cybercriminals.

		Responses		Percent of Cases
		N	Percent	
What network assets within your SMB are key areas targeted by cybercriminals?	Endpoints (e.g., laptops, desktops, mobile devices)	20	15.9%	51.3%
	Servers (e.g., email servers, file servers, web servers)	31	24.6%	79.5%
	Network devices (e.g., routers, switches, firewalls)	15	11.9%	38.5%
	Applications (e.g., web applications, mobile applications)	18	14.3%	46.2%
	Cloud services (e.g., cloud storage, Software-as-a-Service (SaaS) applications)	11	8.7%	28.2%
	Data (e.g., customer data, financial data, intellectual property)	15	11.9%	38.5%
	User accounts (e.g., employee login credentials, administrator accounts)	14	11.1%	35.9%
	Physical infrastructure (e.g., HVAC systems, security cameras)	2	1.6%	5.1%
Total		126	100.0%	323.1%

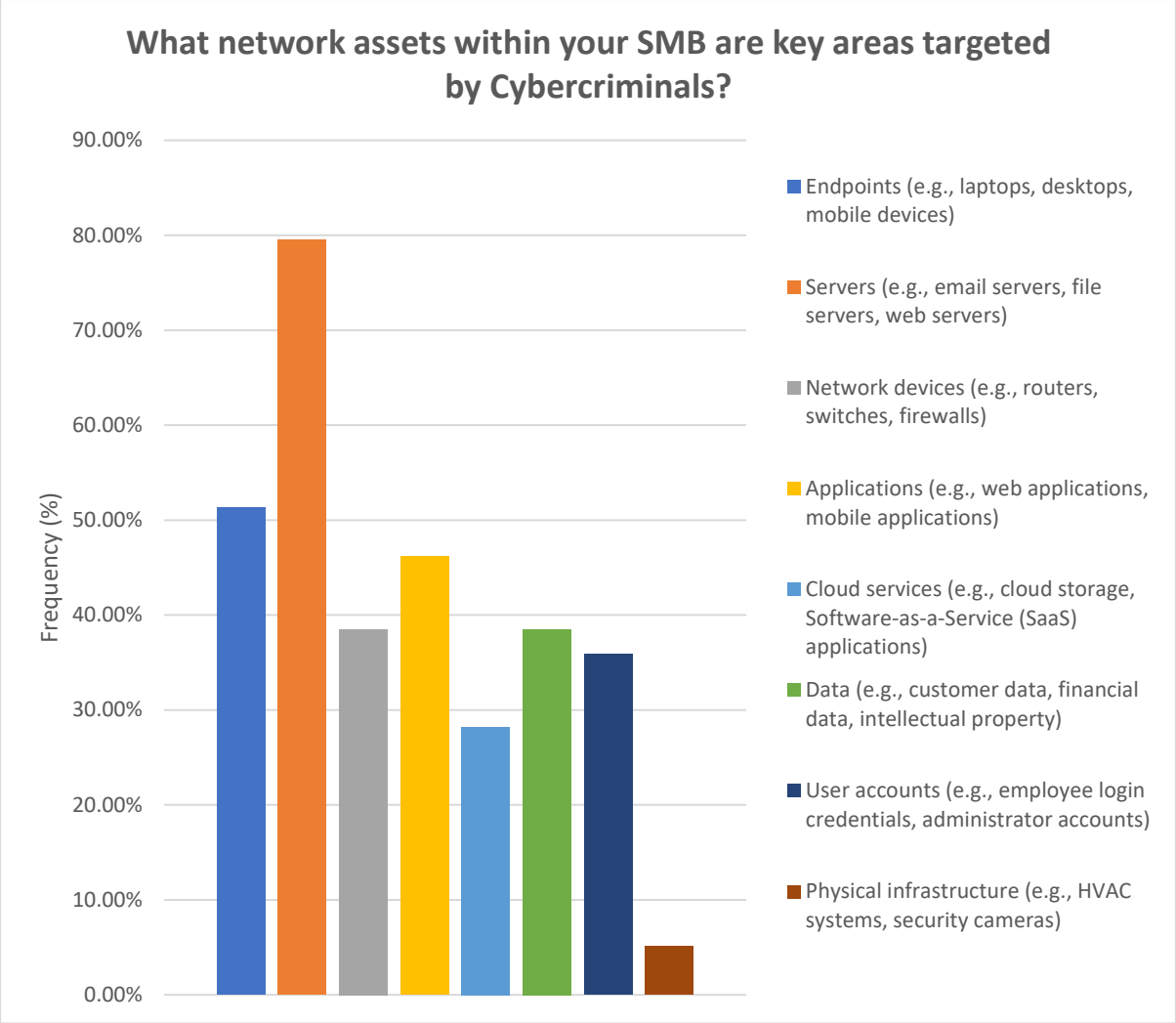

Figure 4- 8 Graph of Network asset within SMBs targeted by Cybercriminals.

Data from Table 4.4 were visualized in Figure 4.8 which shows that Servers are the most attacked network assets within SMBs with almost 80% of respondents supporting this claim. This is followed by Cloud Services with a bit above 50%. Physical Securities are the least attacked network with about 5%.

4.3 What vulnerabilities do these Cybercriminals exploit to gain access to your SMB's network assets?

Table 4.5: Case Summary of Vulnerabilities exploited by Cybercriminals to gain access to SMBs network assets.

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent

What vulnerabilities do these cybercriminals exploit to gain access to your SMB's network assets?	39	84.8%	7	15.2%	46	100.0%
a. Dichotomy group tabulated at value 1.						

Table 4.6: Table showing multiple response analysis result of Vulnerabilities exploited by Cybercriminals to gain access to SMBs network assets.

		Responses		Percent of Cases
		N	Percent	
What vulnerabilities do these cybercriminals exploit to gain access to your SMB's network assets?	Unpatched software vulnerabilities in operating systems, applications, or plugins.	12	8.6%	30.8%
	Weak or easily guessable passwords for user accounts	15	10.7%	38.5%
	Lack of Multi-factor authentication (MFA) on user accounts or devices	14	10.0%	35.9%
	Outdated software or hardware that is no longer supported by the vendor.	12	8.6%	30.8%
	Phishing attacks	25	17.9%	64.1%
	Malware Infections	7	5.0%	17.9%
	SQL injection attacks	8	5.7%	20.5%
	Cross-site scripting (XSS) attacks	3	2.1%	7.7%
	Social engineering attacks	8	5.7%	20.5%
	Unsecured network configurations	6	4.3%	15.4%
	Unsecured cloud services	3	2.1%	7.7%
	Insider threats	10	7.1%	25.6%
	Third-party software and services	8	5.7%	20.5%

	Man-in-the-middle (MitM) attacks	5	3.6%	12.8%
	Insufficient physical security measures	2	1.4%	5.1%
	Prefer not to say	2	1.4%	5.1%
Total		140	100.0%	359.0%

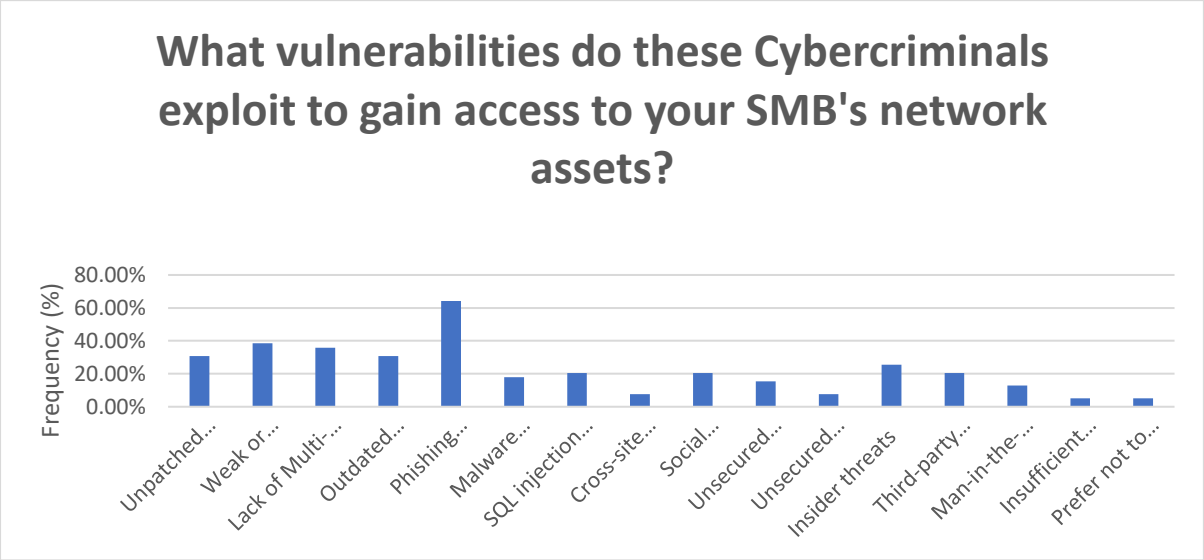

Figure 4- 9 Graph showing Vulnerabilities exploited by Cybercriminals to gain access to SMBs network assets.

Data from Table 4.6 were visualized in Figure 4.9 which shows SMB's network assets with phishing attacks vulnerabilities as the most exploited with about 65%, this is followed by networks that are weak or easily guessable password for user accounts with 38.5% and lack of multi-factor authentication on user accounts with about 35%. Insufficient physical security measures and other vulnerabilities deliberately not mentioned by respondents have the lowest percentage of 5.1%.

4.4 Which of the following measures is a cost-effective and quick solution for your SMB to protect their network assets from Cyber-attacks?

Table 4.7: Case Summary of cost-effective and quick solution for SMB to protect their network assets from Cyber-attacks.

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Cost effective and quick solution	39	84.8%	7	15.2%	46	100.0%
a. Dichotomy group tabulated at value 1.						

Table 4.8: Multiple Response analysis result of cost-effective and quick solution for SMB to protect their network assets from Cyber-attacks.

		Responses		Percent of Cases
		N	Percent	
Which of the following measures is a cost-effective and quick solution for your SMB to protect their network assets from cyber-attacks?	Implementing anti-virus and anti-malware software	21	22.1%	53.8%
	Conducting regular software updates and patches	22	23.2%	56.4%
	Using strong passwords and multi-factor authentication	27	28.4%	69.2%
	Providing cybersecurity training for employees	22	23.2%	56.4%
	Other (Please specify)	3	3.2%	7.7%
Total		95	100.0%	243.6%

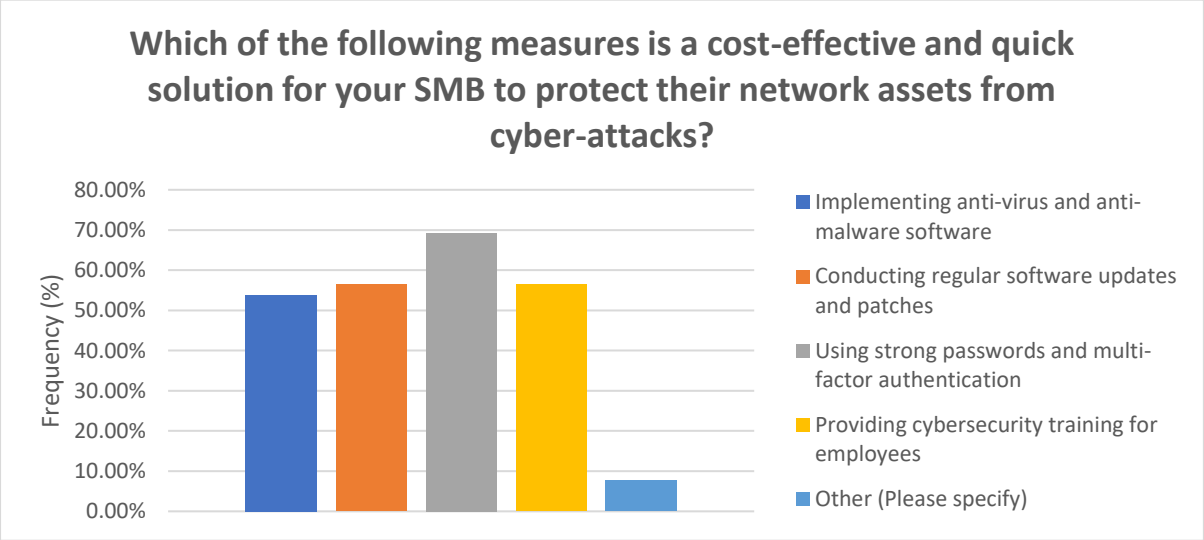

Figure 4- 10 Graph showing cost-effective and quick solution for your SMB to protect their network assets from cyber-attacks.

Data from Table 4.8 were visualized in Figure 4.10 showing About 70% of respondents which is also the highest recorded chose using of strong passwords and multi-factor authentication as a cost effective and quick solution for SMB to protect their networks assets from cyber-attacks. Other cost-effective and quick solutions, not among the listed options make up the least percentage.

4.5 What preventive security measures/mechanisms have your SMB implemented to mitigate Cyberthreats?

Table 4.9: Case Summary of preventive security measures/mechanisms SMB implemented to mitigate Cyberthreats.

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
What preventive security measures/mechanisms have your SMB implemented to mitigate cyber threats?	39	84.8%	7	15.2%	46	100.0%
a. Dichotomy group tabulated at value 1.						

Table 4.10: Multiple Response Analysis result for preventive security measures/mechanisms SMB implemented to mitigate Cyberthreats

		Responses		Percent of Cases
		N	Percent	
What preventive security measures/mechanisms have your SMB implemented to mitigate cyberthreats?	Security information and event management systems (SIEM)	17	15.3%	43.6%
	Multi-factor authentication (MFA)	27	24.3%	69.2%
	Regular software updates and patching	25	22.5%	64.1%
	Employee cybersecurity training	17	15.3%	43.6%
	Encryption and secure data storage	12	10.8%	30.8%
	Network monitoring and intrusion detection	12	10.8%	30.8%
	Other (please specify)	1	0.9%	2.6%
Total		111	100.0%	284.6%

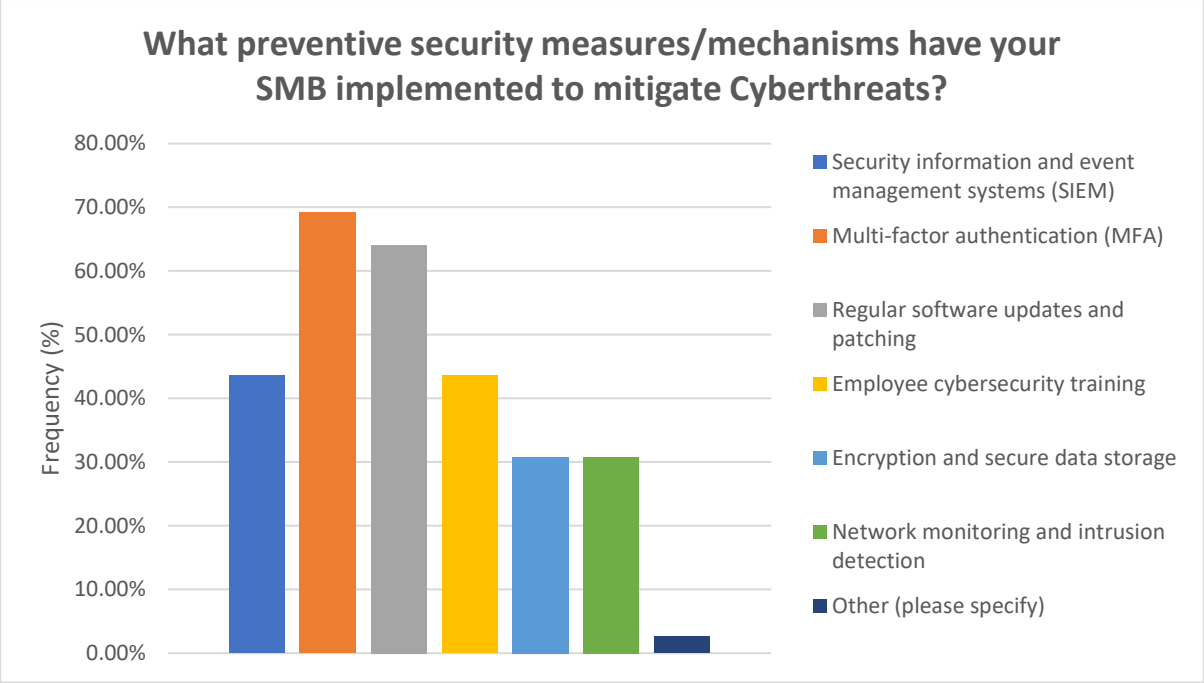

Figure 4- 11 Graph of preventive security measures/mechanisms SMB implemented to mitigate Cyberthreats

Figure 4.11 was visualized using data from Table 4.10, it shows MFA and Regular software updates and patching as the two most widely implemented security measures to mitigate Cyber-threat.

4.6 Rank of challenges SMBs face in managing Cyber Threats in order of significance

Table 4- 11`: Frequency table of Rank of challenges SMBs face managing Cyberthreats in order of significance.

Options/Rank	1	2	3	4	5
Lack of resources	30.6	33.3	22.2	11.1	28
Lack of cybersecurity expertise	25	25	11.1	25	13.9
Limited budget	22.2	27.8	33.3	8.3	8.3
Insufficient time	5.6	5.6	11.1	38.9	38.8
Complexity of cybersecurity measures	16.7	8.3	22.2	16.7	36.1

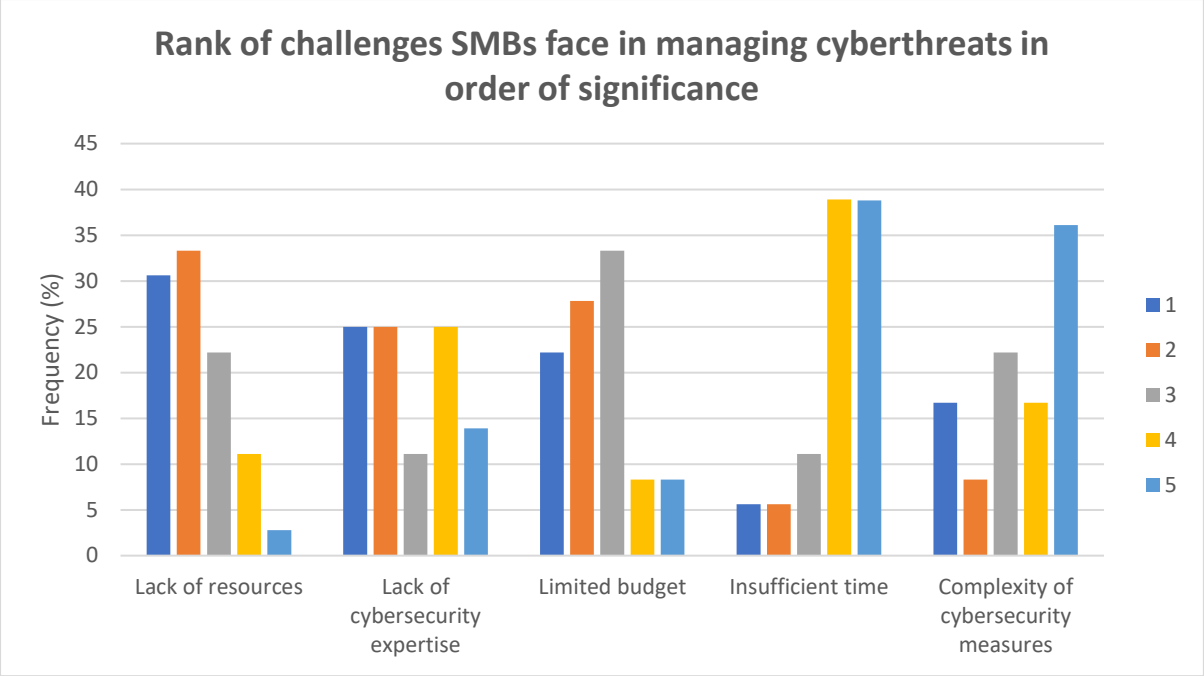

Figure 4- 12 Graph showing rank of challenges SMBs face in managing Cyberthreats.

From Figure 4.12 above showing respondents' rank selections on a scale of 1 to 5 with 1 being the most significant and 5 being the least significant, lack of resources, lack of cybersecurity expertise and limited budget rank highest in terms of significance amongst the other challenges considered by respondents, while insufficient time and complexity of cybersecurity measures rank the least.

"Lack of resources" being one of the most significant according to their frequency is cross tabulated with "which industry does organization belong to" and the resulting Chi-Square analysis result table provided below in the table below.

		Which industry does your organization belong to? - Selected Choice						Total
		Information Technology	Finance	Healthcare	Retail	Manufacturing	Education	
	Most Significant (1)	3	4	0	0	1	3	11
	Moderately Significant (2)	6	1	0	1	1	3	12
	Neutral (3)	4	2	1	1	0	0	8
	Low Significant (4)	3	0	0	0	0	1	4

	Least Significant (5)	0	0	0	0	0	1	1
Total		16	7	1	2	2	8	36

Crosstabulation of - Lack of resources * Which industry does your organization belong to? - Selected Choice

Table 4- 12 *Crosstabulation of "lack of resources" and "which industry does your organization belong to"*

		Which industry does your organization belong to? - Selected Choice						Total
		Information Technology	Finance	Healthcare	Retail	Manufacturing	Education	
	1	3	4	0	0	1	3	11
	2	6	1	0	1	1	3	12
	3	4	2	1	1	0	0	8
	4	3	0	0	0	0	1	4
	5	0	0	0	0	0	1	1
Total		16	7	1	2	2	8	36

Table 4.13 shows the Chi-Square analysis result of "lack of resources" and "which industry does your organization belong to"

Chi-Square Tests

Table 4.13- Chi-Square analysis result of "lack of resources" and "which industry does your organization belong to"

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	16.702[a]	20	.672
Likelihood Ratio	19.300	20	.502
Linear-by-Linear Association	.137	1	.711
N of Valid Cases	36		

The P-values 0f 0.672 from the Chi-Square analysis shows no statistically significant relationship between lack of resources and the organization industry type.

4.7 Rate of preventive security measures for SMB according to importance

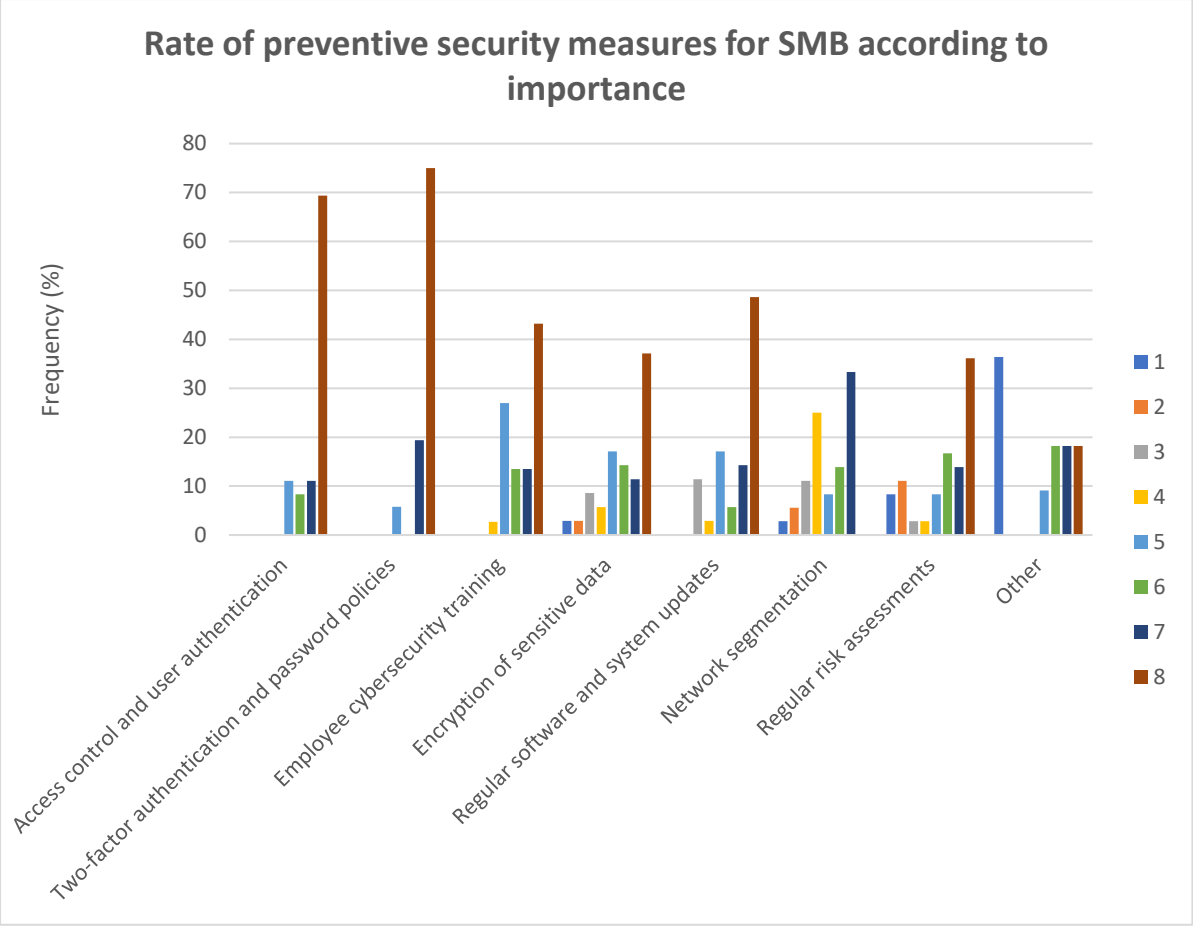

Figure 4- 13 Graph showing rate of preventive security measures for SMB.

From Figure 4.13, Preventive security measures are rated with 1 being the least important and 8 being the most important.

In the listed preventive security measures for SMB, the largest percentage of respondents rated Access control and user authentication, Two-factor authentication and password policies and finally Regular software and system updates as the most important.

Focusing on "Access control and user authentication" because of its high frequency from respondents, a crosstabulation of it with "Has your organization experience a cyber threat or attack" is done and resulting a Chi-square analysis result tabulated.

Crosstabulation - Access control and user authentication * Has your organization ever experienced a cyber threat or attack?

Table 4- 15 *Crosstabulation of "Access control and user authentication" and "Has your organization ever experience a cyber threat or attack"*

	Has your organization ever experienced a cyber threat or attack? - Selected Choice		Total
	No	Yes (Please provide more details)	

	5	4	0	4
	6	2	1	3
	7	3	1	4
	8	19	6	25
Total		28	8	36

Chi-Square Tests

Table 4-16: *Chi-Square analysis result of "Access control and user authentication" and "Has your organization ever experience cyber threat or attack"*

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	1.421[a]	3	.701
Likelihood Ratio	2.267	3	.519
Linear-by-Linear Association	.521	1	.471
N of Valid Cases	36		

The Chi-Square P-value of 0.701 indicate no statistically significant relationship between "access control and user authentication" and Organization with cyber threat experience.

5. Project Evaluation

This section carefully evaluates the research objectives, in relation to the analytical feedback from the previous chapter of this research. This step helps to propose working recommendations as documented in section 6 of this research.

5.1 Objectives Review

The objectives of this research were carefully designed to achieve a comprehensive understanding of the factors and impacts of cybercrime on small and medium businesses (SMBs) and propose strategies to enhance their cybersecurity. Let's evaluate each objective in light of the research findings and the research question.

Objective 1: Gain a deeper understanding of the types of threat caused by cybercrime to SMBs.

The research extensively analyzed various cyber threats faced by SMBs, with phishing attacks and insider threats identified as the most significant ones.

Findings from Chapter 4 provide valuable insights into the prevalence and nature of cyber threats, which have contributed to fulfilling this objective.

Objective 2: Analyse the factors that lead to cybercrime against SMBs.

The research thoroughly examined the factors that contribute to cybercrime incidents targeting SMBs. Vulnerabilities such as unpatched software, weak passwords, and lack of multi-factor authentication were highlighted as key factors exploited by cybercriminals.

Chapter 4 provided detailed discussions on the factors leading to cybercrime, aligning with the objective of the study.

Objective 3: Propose an emerging technology to provide a more secure digital environment for SMBs.

The proposed framework in Chapter 6, which includes recommendations based on the analyzed data and respondents' feedback, addresses this objective.

The integration of Artificial Intelligence (AI) into the cybersecurity framework demonstrates a forward-looking approach to enhance SMBs' defense against cyberattacks.

Research Question: How can cyberattacks on SMBs be curtailed effectively?

The research findings and the proposed framework in Chapter 6 provide comprehensive answers to the research question by offering practical strategies and preventive measures to mitigate cyber threats effectively.

5.2 Evaluation of Methodology and Results

This section is important so that a systematic framework can be proposed for the SMBs to implement in their organisation. This will start with the critical evaluation of the methodology of this research, then it will proceed with the critical evaluation of the results of the data analysis.

5.2.1 Evaluation of Methodology

The chosen research methodology provides a structured and systematic approach to investigating the factors contributing to cybercrime against small and medium-sized businesses (SMBs). The evaluation of the methodology employed in this study is as follows:

Firstly, the use of a quantitative research design is deemed appropriate for research objectives as it enables the collection of numerical data necessary for analyzing relationships and drawing statistical inferences. This is achieved through a survey-based approach that utilizes a structured questionnaire, facilitating the collection of standardized data from a large sample of SMBs.

The sample selection process which employs a purposive sampling technique to ensure that participants possess knowledge and experience in internet usage and cybersecurity was considered. The total number of 48 responses were gathered due to the complexity of the research time.

The data collection procedure involves the utilization of a self-administered online questionnaire developed through Qualtrics. The questionnaire is designed to facilitate efficient data collection and undergoes pilot testing to ensure clarity, comprehensibility, and reliability. Adjustments are made based on the results of the pilot study, further improving the final survey instrument.

The comprehensive data analysis is ensured through the use of appropriate statistical techniques, including descriptive statistics and inferential analyses. Descriptive statistics summarize participant characteristics, while inferential analyses such as chi-square tests and regression analysis address the research questions and explore relationships between variables. Statistical software like SPSS and Tableau is employed to support accurate analysis and proper visualization.

On the similar note, the measurement of variables is carefully considered, with appropriate measurement scales selected to capture the nuances and variations within the research aims. Categorical scales, Likert scales, and a combination of both are employed to measure cybercrime incidents, vulnerabilities, cybersecurity measures, and the impact of cybercrime. This selection of measurement scales ensures reliable and meaningful data collection.

Finally, the reliability and validity of the research instrument are given due attention. The use of validated Qualtrics software, careful examination by the supervisor, and implementation of improvements based on feedback enhance the validity of the questionnaire. Reliability tests, such as Cronbach's alpha, are conducted to assess the instrument's consistency and performance.

5.2.2 Evaluation of Results

As presented in chapter 4 of this research, the most significant cyber-threat affecting SMBs is Phishing Attacks, although Insider Threat and Social Engineering are still significant threats but not as Phishing attacks. These cyber-threats are majorly targeted at servers, cloud services and applications which show phishing attack vulnerabilities, weak or easily guessable password for user account or lack of multi-factor authentication of user account. Highly rank preventive security measures/mechanism like Multi-Factor Authentication and Regular Software updates are commonly implemented to mitigate these threats, other preventive measures like Security Information and Event Management systems (SIEM) and Employee Cybersecurity Training are also reasonably rank in users' awareness and use. Most times, these preventive measures have some significant challenges militating against them, the most significant of these challenges are lack of resources, lack of cybersecurity expertise and limited budget.

As shown in Fig. 4.4, most of the respondents are IT specialists. This shows that over 75% of the respondents should be able to seamlessly integrate the proposed framework in their organisation. Because they hardly experience cyber-attacks (Fig. 4. 6), this does not mean that the organisation should not implement the proposed framework since most have them have more than 3 years' experience (Fig 4.5).

Since Phishing attacks, insider threats, social engineering, and the distributed denial of service (DDoS) attacks tops the chart (Fig 4.8), this means that the proposed framework must critically consider these types of attacks.

Due to the cost effectiveness, Figure 4.10 shows that, many SMBs are familiar and agree that the use of strong password and the multi-factor authentication system, proper cyber-security training for the employees, conduction of regular software updates and patches and the

implementation of the antivirus and the anti-malware software can greatly help to mitigate the effect of cyber-attacks.

Although security information and event management (SIEM) are one of the known security measures against the cyber-attacks, many still relies on the multi-factor authentication (MFA) and the regular software updates. However, over 40% have started considering the SIEM and see the need for training employees on cyber-security as crucial (Fig 4.11).

It can also be pointed out that basic resource availability contributes heavily to the challenges the SMBs face in managing the cyber-threats. There are mixed opinions on the availability of the cyber-security expertise are the issue with the SMBs to combat the cyber-threats. These mixed opinions may be as personal preference that some believe that if they have enough resources, they can easily higher security experts to improve their systems while others may believe that if there are enough resources, they should have permanent security worker that can be reached at any time. This choice is purely based on company's preference. A very high percentage disagreed that the time can be the reason not to consider proper steps to mitigate the cyber-attacks while there seems to be a mixed opinion on the view when it comes to the complexity of cyber-security (fig 4.12).

Lastly, access control and user authentication, two-factor authentication and password policies, the need for training employees for cyber-security professions, sensitive data encryption, regular software and system updates, regular risk assessment and other security preventive measures seems to be of importance.

5.4 Evaluation of Ethical, Legal, Social, Security, And Professional Considerations

Throughout the research process, it is crucial to evaluate and address various ethical, legal, social, security, and professional considerations to ensure the integrity and validity of the study. This section discusses the evaluation of these.

5.4.1. Ethical Considerations

Ethical considerations play a fundamental role in research, especially when dealing with sensitive topics such as cybercrime. The following ethical principles were upheld during the research:

- Informed Consent: Prior to data collection, participants were provided with clear information about the research objectives, procedures, and potential risks and benefits. Informed consent was obtained, ensuring that participants voluntarily agreed to participate and had the freedom to withdraw at any time.
- Confidentiality and Anonymity: Measures were taken to ensure the confidentiality and anonymity of the participants. All data collected was kept confidential, and participant identities were protected. Any personal identifying information was removed or anonymized during the analysis and reporting of the data.
- Data Protection: Data protection regulations and best practices were followed to safeguard the participants' personal information. Appropriate measures were implemented to secure the data, such as encryption and restricted access.

- Avoiding Harm: Steps were taken to minimize any potential harm or distress to participants. The research design and data collection methods were carefully planned to ensure that participants' well-being and privacy were protected.

5.4.2. Legal Considerations

Adherence to legal requirements and regulations is crucial in conducting research. In the context of cybersecurity research, the following legal considerations were evaluated:

- Data Protection Laws: Compliance with relevant data protection laws and regulations, such as the General Data Protection Regulation (GDPR) or the Data Protection Act, was ensured. Participants' data was collected and handled in accordance with these laws, ensuring the lawful and fair processing of personal information.
- Intellectual Property Rights: Proper acknowledgement and citation of sources were maintained to respect intellectual property rights. Any copyrighted material, such as images or text, was appropriately credited or obtained with permission.

5.4.3. Social Considerations

The research on cybercrime and its impact on SMBs has important social implications. Understanding and addressing social considerations is vital to ensure that the research is relevant and beneficial to society. Some social considerations evaluated include:

- Social Impact: The findings and recommendations of the research aim to contribute to the protection and resilience of SMBs against cybercrime. By enhancing cybersecurity measures, the research strives to mitigate the negative impact of cybercrime on SMBs, their stakeholders, and the wider community.
- Equity and Accessibility: Efforts were made to ensure that the research was inclusive and accessible to a diverse range of SMBs. The research design and data collection methods were developed in a way that minimized any potential barriers or biases, allowing for equal participation and representation.

5.4.4. Security Considerations

Given the nature of the research topic, security considerations were carefully evaluated to protect the integrity and confidentiality of the research process and data. These considerations included:

- Data Security: Robust data security measures were implemented to protect the collected data from unauthorized access, breaches, or data loss. This involved encryption, restricted access, and secure storage methods.
- Participant Privacy: The privacy and confidentiality of participants' data were prioritized throughout the research. Steps were taken to ensure that participants' personal information was not disclosed or compromised.

5.4.5. Professional Considerations

Maintaining professional standards and practices is essential in research. The research followed professional guidelines and considerations, including:

- Rigor and Validity: The research adhered to rigorous methods and analysis techniques to ensure the validity and reliability of the findings. The use of appropriate statistical analysis tools and adherence to academic research standards were followed.
- Academic Integrity: Proper citation and acknowledgement of sources were maintained to uphold academic integrity. Plagiarism and any forms of misconduct were strictly avoided.
- Peer Review: Where applicable, the research underwent a peer review process to obtain expert feedback and ensure the quality and credibility of the study.
- Conflict of Interest: Any potential conflicts of interest were identified and addressed to maintain the objectivity and impartiality of the research.

By thoroughly evaluating these ethical, legal, social, security, and professional considerations, the research upholds the highest standards of integrity, respects the rights and privacy of participants, and contributes positively to the field of cybersecurity.

6. Conclusion, Recommendation and Future Studies

This section documents the general conclusion of the study, the conclusion also covers the points from the recommendation and the future studies section. The next section 6.2 provides the recommendation of this study. This is the section which documents the proposed recommendations after careful analysis of the respondents' feedback. This chapter is concluded by documenting the area which can be available for future research.

6.1 Conclusion

This section documents the general conclusion of this research.
This research findings which proves that the phishing attacks and insider threats are the most identified as the most prominent threats, are congruent with the existing literature in the academic domain (Saxena et.al, 2020; Verizon, 2019). The literature review extensively underscores the significance of phishing attacks and insider threats as major cyber risks targeting SMBs, and the research outcomes substantiate and reinforce these established findings.

Furthermore, the identification of servers, cloud services, and applications as primary targets of cybercriminals within SMBs is in consonance with the scholarly literature (Alahmari & Duncan, 2020). Studies by Alahmari & Duncan (2020) and Mishra et al (2022), have consistently emphasized that cybercriminals frequently direct their efforts towards compromising these critical network assets due to their pivotal role in SMB operations and their potential for accessing valuable data.
Likewise, the research's outcome concerning the vulnerabilities exploited by cybercriminals, including unpatched software, weak passwords, and the absence of multi-factor authentication, aligns cohesively with the existing academic literature (Australian Government, 2021). Prior research has repeatedly underscored these vulnerabilities as significant weak points that malicious actors exploit to gain unauthorized access to SMBs' information systems (University of Maryland, 2019; Australian Government, 2021).

In response to these threats, the research suggests cost-effective and quick solutions for SMBs to protect their network assets from cyber-attacks. Measures such as implementing strong

passwords and multi-factor authentication, conducting regular software updates and patches, and providing cybersecurity training for employees are recommended as effective preventive measures.

Furthermore, the research evaluates the challenges faced by SMBs in managing cyber threats, with limited resources, lack of cybersecurity expertise, and budget constraints identified as significant challenges. The importance of addressing these challenges and providing tailored solutions for SMBs is emphasized.

Based on the evaluation of the methodology and results, the research provides a systematic framework for SMBs to enhance their cybersecurity. This framework includes components such as employee education and awareness, strict access control, regular software and system updates, encryption of critical data, and ongoing risk assessment.

The research also addresses various ethical, legal, social, security, and professional considerations to ensure the integrity and validity of the study. Ethical principles, data protection laws, participant privacy, social impact, and security measures were carefully evaluated and adhered to throughout the research process.

In conclusion, the research contributes to the understanding of cybercrime's impact on SMBs and provides practical strategies to enhance their cybersecurity. The findings and proposed framework can be valuable tools for SMBs, policymakers, and cybersecurity experts in their efforts to mitigate cyber threats and create a safe online environment for small and medium-sized businesses.

6.2 Recommendations

The recommendation of this research is based on the critical analysis of the respondent's feedback as documented in section 5.2.2.

6.2.1 Proposed Recommendations for Cybersecurity in SMBs

Based on the analyzed data and the identified needs of SMBs in mitigating cyber-attacks, a high-level professional framework is proposed. This framework aims to provide a systematic approach for SMBs to implement effective cybersecurity measures within their organizations. Figure 6.1 summaries the proposed framework.

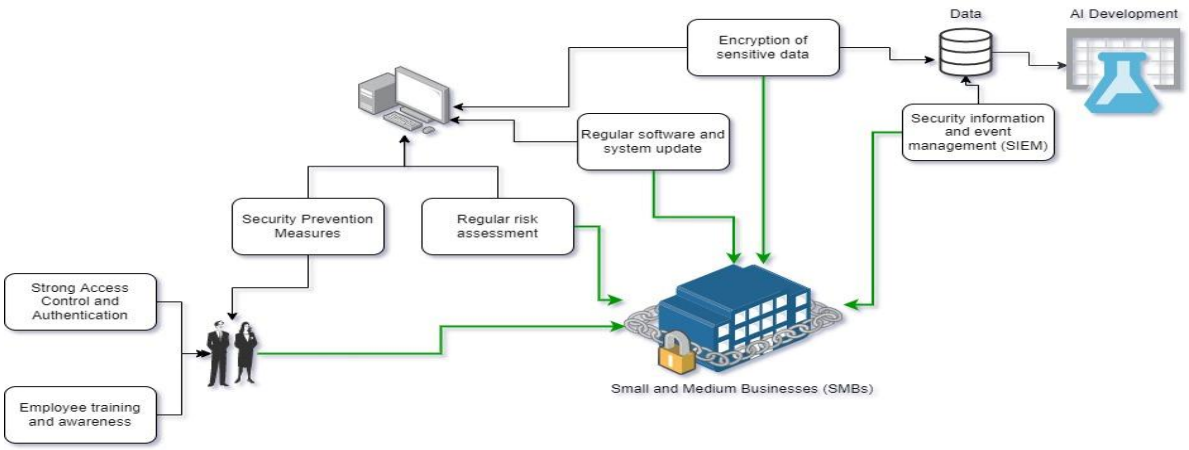

Figure 6- 1 Proposed Framework for the Secured SMBs

This proposed framework incorporates principles derived from Routine Activity Theory (RAT) and the Social Learning Theory (SLT). These theories provide a theoretical foundation for understanding the factors that contribute to cybercrime and offer insights into effective preventive measures (Maimon et.al, 2021; Smith, 2020). The framework comprises the following key elements:

6.2.1.1. Employee Training and Awareness

Drawing on the principles of the Social Learning Theory (SLT), it is important to work on the development of comprehensive cybersecurity training programs for employees. These programs focus on topics such as identifying phishing attacks, recognizing social engineering tactics, understanding of insider threats, and promoting safe online practices. By fostering a culture of awareness and knowledge sharing, SMBs can reduce the opportunities for cybercriminals to exploit vulnerabilities.

The ISO27001, security awareness training policy (Table, 2020a) ensures all employees receive appropriate awareness education and training in all aspects of information security. This ensures that the employees get regular updates in policies and procedures that are relevant to their role (Table 2020a).

6.2.1.2. Strong Access Control and Authentication

Routine Activity Theory (RAT) highlights the importance of controlling access to sensitive systems and data. The framework recommends implementing robust access control mechanisms, including two-factor authentication and strong password policies. Regular review and update of access privileges based on employee roles and responsibilities help minimize the likelihood of unauthorized access and data breaches. By strictly following the security standard by ISO27001 (Table, 2020b) and the risk management provided by ISO/SAE 21434 (Team, 2020), the proper access control can be followed.

6.2.1.3. Regular Software and System Updates

Consistent with RAT, the framework advocates for a proactive approach to software and system updates. By promptly applying security patches and updates, SMBs can address known vulnerabilities and reduce the opportunities for cybercriminals to exploit weaknesses. An automated update process and a schedule for regular patch management ensure that systems are continuously strengthened against emerging threats (Team, 2020).

6.2.1.4. Security Information and Event Management (SIEM)

In alignment with RAT, the framework considers the adoption of Security Information and Event Management (SIEM) solutions to enhance threat detection and incident response capabilities. SIEM tools monitor network activities, identify security incidents, and provide real-time alerts. By leveraging SIEM technology, SMBs can detect and respond to potential cyber threats more effectively, reducing the impact of security breaches. However, from the gathered report, financial capability seems to be the major contribution to the discouragement

on implementing this software, hence, SIEM tool with affordable-yet extensive features should be considered.

Splunk Enterprise Security (Splunk, 2021) is recommended in this situation. This Windows and Linux application is a global leader because it integrates network analysis with log management and an exceptional analysis tool with cheaper price (Keary, 2018).

6.2.1.4.1 Comparative Analysis of SIEM Solutions for SMBs

In addition to recommending Splunk as a potential Security Information and Event Management (SIEM) solution for small and medium-sized businesses (SMBs), it is essential to critically analyze and compare other SIEM options available in the market. While Splunk may be a robust and popular choice, it is vital to consider other SIEM solutions that may offer competitive advantages, better cost-effectiveness, and greater compatibility with SMB requirements.

IBM QRadar: IBM QRadar (IBM, n.d) is a widely recognized SIEM platform known for its advanced analytics capabilities and real-time threat detection. It offers extensive integrations with various security tools and cloud platforms, making it a versatile choice for SMBs with diverse IT infrastructures. Additionally, IBM QRadar provides out-of-the-box content and predefined rules for quick deployment, which can be beneficial for SMBs with limited cybersecurity expertise. However, SMBs must evaluate the total cost of ownership and scalability aspects to ensure it fits within their budget and future growth plans.

SolarWinds Security Event Manager (SEM): SolarWinds SEM (2016) is another SIEM solution that caters to the needs of SMBs. It boasts user-friendly features, making it easier for organizations with limited IT resources to manage security events effectively. SolarWinds SEM offers broad compatibility with various platforms and devices, allowing SMBs to centralize and correlate security logs from multiple sources. Additionally, its licensing model and pricing structure are designed to suit the financial constraints of SMBs. SMBs may find this option attractive due to its affordability and ease of use.

6.3 Future Studies

The research provides valuable insights into the factors and impacts of cybercrime on SMBs. However, there is still room for future research. This section outlines numerous essential areas for further studies. To begin, a mix of questionnaires and interviews would provide deeper insights into the cybersecurity challenges encountered by SMBs. Although the survey-based technique with a structured questionnaire has proven to be beneficial, including open-ended interview questions would improve the study design process. Secondly, keeping up with emerging threat patterns affecting SMBs is critical for continuous research efforts. Furthermore, future research should focus on the role of AI in SMB cybersecurity, considering its potential for reducing new threats and strengthening defense measures. Conducting research in these areas will further enhance will promote a thorough understanding of SMB cybersecurity and contribute to the development of effective solutions for increased resilience against cyber-attacks.

References

1) AAG (2023). The Latest 2023 Cyber Crime Statistics (updated March 2023). Available at: https://aag-it.com/the-latest-cyber-crime-statistics/
2) Abel Yeboah-Ofori & Francisca Afua Opoku-Boateng (2023). Mitigating cybercrimes in an evolving organizational landscape. https://www.emerald.com/insight/content/doi/10.1108/CRR-09-2022-0017/full/html
3) Ahn, J. N., Hu, D., & Vega, M. (2019). "Do as I do, not as I say": Using social learning theory to unpack the impact of role models on students' outcomes in education. Social and Personality Psychology Compass, 14(2), 1–12. https://doi.org/10.1111/spc3.12517
4) Ambika, Dr. T., & Senthilvel, Dr. K. (2020). Cyber Crimes against the State: A Study on Cyber Terrorism in India. Webology, 17(2), 65–72. https://doi.org/10.14704/web/v17i2/web17016
5) Ani Petrosyan (2023). Number of ransomware attacks worldwide from 1st quarter 2020 to 4th quarter 2022. https://www.statista.com/statistics/1315826/ransomware-attacks-worldwide/
6) Australian Government. (2021, August 3). Protect your business from cyber threats | business.gov.au. Business.gov.au. https://business.gov.au/online/cyber-security/protect-your-business-from-cyber-threats
7) Back, S., & LaPrade, J. (2020). Cyber-Situational Crime Prevention and the Breadth of Cybercrimes among Higher Education Institutions. International Journal of Cybersecurity Intelligence & Cybercrime, 3(2), 25–47. https://vc.bridgew.edu/ijcic/vol3/iss2/3/
8) Bender-Salazar, R. (2023). Design thinking as an effective method for problem-setting and needfinding for entrepreneurial teams addressing wicked problems. Journal of Innovation and Entrepreneurship, 12(1). https://doi.org/10.1186/s13731-023-00291-2
9) Bello, M., & Griffiths, M. (2020). Routine Activity Theory and Cybercrime Investigation in Nigeria: How Capable Are Law Enforcement Agencies? Rethinking Cybercrime, 213–235. https://doi.org/10.1007/978-3-030-55841-3_11
10) CESER (2021). C2M2, version 2.0. https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021_508.pdf
11) Chris Sylvester (2018). Your Small Business's Greatest Cybersecurity Threat Comes from Inside.. Network Depot. https://www.networkdepot.com/small-business-insider-threats/
12) Cloudian. (n.d.). Splunk Architecture: Components and Best Practices. Cloudian. Retrieved July 13, 2023, from https://cloudian.com/guides/splunk-big-data/splunk-architecture-data-flow-components-and-topologies/#:~:text=Splunk%20gathers%20logs%20by%20monitoring
13) Daniel, K., & Andreas, J. (2022). Evaluation of AI-based use cases for enhancing the cyber security defense of small and medium-sized companies (SMEs). Electronic Imaging, 34(3), 387–381387–388. https://doi.org/10.2352/ei.2022.34.3.mobmu-387
14) Eybers, S., & Mvundla, Z. (2021). Investigating Cyber Security Awareness (CSA) Amongst Managers in Small and Medium Enterprises (SMEs). Comprehensible Science, 180–191. https://doi.org/10.1007/978-3-030-85799-8_16
15) Fahlevi, M., Saparudin, M., Maemunah, S., Irma, D., & Ekhsan, M. (2019). Cybercrime Business Digital in Indonesia. E3S Web of Conferences, 125(21001), 21001. https://doi.org/10.1051/e3sconf/201912521001

16) Ho, Mr. H., Ko, P. R., & Mazerolle, P. L. (2022). Situational Crime Prevention (SCP) Techniques to Prevent and Control Cybercrimes: A Focused Systematic Review. Computers & Security, 115, 102611. https://doi.org/10.1016/j.cose.2022.102611
17) IBM (2019). Cost of data breach report. https://www.ibm.com/downloads/cas/RDEQK07R
18) Idem, U. J., Olarinde, E. S., Ikpeze, N. G., Anwana, Emem, O., Ogundele, A. T., & Awodiran, M. A. (2023). Cybercrime Regulatory Agencies need urgent Reform to Protect Nigeria. 2023 International Conference on Cyber Management and Engineering (CyMaEn). https://doi.org/10.1109/cymaen57228.2023.10050994
19) João, A., Plesker, C., Klaus Schützer, Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. Electronics, 12(8), 1920–1920. https://doi.org/10.3390/electronics12081920
20) Keary, T. (2018). 9 Best SIEM Tools: A Guide to Security Information and Event Management. Comparitech.com. https://www.comparitech.com/net-admin/siem-tools/
21) Kergroach, S., Becker, S., Bernat, L., & Bernat, S. K., Stefan Becker and Laurent. (2022, March 14). Shielding SMEs – how to boost their defence against cyberattacks - Cogito. Oecdcogito.blog. https://oecdcogito.blog/2022/03/14/shielding-smes-how-to-boost-their-defence-against-cyberattacks/
22) Koteshwar, M., & Singh, B. B. J. (2019). Survey Report on Cyber Crimes and Cyber Criminals Get Protected from Cyber Crimes Review Paper. International Journal of Computer Sciences and Engineering, 7(12), 99–109. https://doi.org/10.26438/ijcse/v7i12.99109
23) Lee, C. S., & Wang, Y. (2022). Typology of Cybercrime Victimization in Europe: A Multilevel Latent Class Analysis. Crime & Delinquency, 001112872211188. https://doi.org/10.1177/00111287221118880
24) Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7(7), 8176–8186. Sciencedirect. https://doi.org/10.1016/j.egyr.2021.08.126
25) Lionel Sujay Vailshery (2023). Year-over-year (YoY) increase in open source software (OSS) supply chain attacks worldwide from 2020 to 2022. https://www.statista.com/statistics/1268934/worldwide-open-source-supply-chain-attacks/
26) Maimon, D., Howell, C. J., Perkins, R. C., Muniz, C. N., & Berenblum, T. (2021). A Routine Activities Approach to Evidence-Based Risk Assessment: Findings From Two Simulated Phishing Attacks. Social Science Computer Review, 089443932110463. https://doi.org/10.1177/08944393211046339
27) Mittal, S., & Ilavarasan, P. V. (2019). Demographic Factors in Cyber Security: An Empirical Study. Lecture Notes in Computer Science, 667–676. https://doi.org/10.1007/978-3-030-29374-1_54
28) National Cyber Security Alliance. (2019). Small Business Cybersecurity Survey. Retrieved from https://staysafeonline.org/wp-content/uploads/2019/10/2019-NCSA-SMB-Security-Report.pdf
29) NCSC (2019). Annual Review. https://www.ncsc.gov.uk/annual-review/2019/ncsc/docs/ncsc_2019-annual-review.pdf
30) Neufeld, D. (2023). Computer crime motives: Do we have it right? Sociology Compass, 17(4). https://doi.org/10.1111/soc4.13077

31) Neufeld, D. (2023). Computer crime motives: Do we have it right? Sociology Compass. https://doi.org/10.1111/soc4.13077
32) Niko Bender (2018). Two Sides of DDoS Attacks: The Largest Attack of All Time and Focus on SMEs. https://www.dotmagazine.online/issues/economic-engine-digital-infrastructure/interconnected-digital-world/two-sides-of-ddos-attacks
33) Noche, E. B. (2021). A Literature Review of Empirical Studies on Cyber Security Workforce Development. Asian Journal of Multidisciplinary Studies, 4(2), 65–73. https://www.asianjournal.org/online/index.php/ajms/article/view/346
34) Paoli, L., Visschers, J., & Verstraete, C. (2018). The impact of cybercrime on businesses: a novel conceptual framework and its application to Belgium. Crime, Law and Social Change, 70(4), 397–420. https://doi.org/10.1007/s10611-018-9774-y
35) Pedreira, V., Barros, D., & Pinto, P. (2021). A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0 with New Challenges on Data Sovereignty Ahead. Sensors, 21(15), 5189. https://doi.org/10.3390/s21155189
36) Raja, N. M., & Vegad, S. (2023). An empirical study for the traffic flow rate prediction-based anomaly detection in software-defined networking: a challenging overview. Social Network Analysis and Mining, 13(1). https://doi.org/10.1007/s13278-023-01057-0
37) Robin Materese (2018). Small Business Cybersecurity Corner. NIST. https://www.nist.gov/itl/smallbusinesscyber
38) Saridakis, G., Benson, V., Ezingeard, J.-N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. Technological Forecasting and Social Change, 102, 320–330. https://doi.org/10.1016/j.techfore.2015.08.012
39) Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.-K. R., & Burnap, P. (2020). Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. Electronics, 9(9), 1460. https://doi.org/10.3390/electronics9091460
40) Sikra, J., Renaud, K. V., & Thomas, D. R. (2023). UK cybercrime, victims and reporting : a systematic review. Commonwealth Cybercrime Journal, 1(1), 28–59. https://strathprints.strath.ac.uk/84979/
41) Smith, M. A. (2020). Social Learning and Addiction. Behavioural Brain Research, 398(1), 112954. https://doi.org/10.1016/j.bbr.2020.112954
42) Splunk. (2021). Splunk Validated Architectures. https://www.splunk.com/en_us/pdfs/tech-brief/splunk-validated-architectures.pdf
43) Statista. (2023a). Annual number of malware attacks worldwide from 2015 to 2022. Statista. https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/
44) Statista (2021). Global distributed denial of service (DDoS) attacks worldwide in 2021, by attacked country. https://www.statista.com/statistics/1255583/ddos-attacks-by-attacked-country/
45) Statista (2022a). Distribution of cyber attacks across worldwide industries in 2022. https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/
46) Statista (2022b). Distribution of web application critical vulnerabilities worldwide as of 2022. https://www.statista.com/statistics/806081/worldwide-application-vulnerability-taxonomy/

47) Statista (2022c). Industry sectors most frequently targeted by malware attacks worldwide from July 2022 to August 2022. https://www.statista.com/statistics/1326618/industry-sectors-targeted-by-malware-attacks-worldwide/
48) Statista (2023b). Phishing attack volume in global companies 2021. https://www.statista.com/statistics/1149241/share-organizations-worldwide-phishing-attack/#:~:text=Phishing%20attack%20rate%20among%20businesses%20worldwide%202021&text=A%202021%20survey%20revealed%20that
49) Symantec. (2016). Internet Security Threat Report. https://
50) www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
51) Table, H. (2020a, April 14). ISO 27001 Security Awareness Training Policy Ultimate Guide. High Table. https://hightable.io/iso27001-security-awareness-training-policy-template-beginners-guide/#:~:text=The%20ISO%2027001%20Security%20Awareness%20Training%20Policy%20is%20to%20ensure
52) Table, H. (2020b, August 17). ISO 27001 Access Control Policy Ultimate Guide. High Table. https://hightable.io/iso-27001-access-control-policy-ultimate-guide/#:~:text=The%20ISO%2027001%20Access%20Control%20Policy%20ensures%20the%20correct%20access
53) Tawalbeh, L., Darwazeh, N. S., Al-Qassas, R. S., & AlDosari, F. (2015). A Secure Cloud Computing Model based on Data Classification. Procedia Computer Science, 52, 1153–1158. https://doi.org/10.1016/j.procs.2015.05.150
54) Team, A. A. T. (2020, March 25). Complete List of Cyber Security Standards (Updated 2021). All about Testing. https://allabouttesting.org/complete-list-of-cyber-security-standards/
55) Tessian (2022). Insider Threat Statistics You Should Know: Updated 2022. https://www.tessian.com/blog/insider-threat-statistics/
56) University of Maryland. (2019). Small Business Cybersecurity Survey. https://www.umgc.edu/content/dam/umgc/documents/upload/maryland-cybersecurity-council-activities-report-2017-2019.pdf
57) Verison (2019). Shut down insider threats. https://www.verizon.com/business/resources/reports/insider-threat-report/
58) Verizon (2022). Data Breach Investigations Report. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/
59) World Bank (2023). Small and Medium Enterprises (SMEs) Finance. Available at: https://www.worldbank.org/en/topic/smefinance#:~:text=SMEs%20account%20for%20the%20majority,(GDP)%20in%20emerging%20economies