Challenges of implementing cybersecurity and data protection measures in Small and Medium Enterprises (SMEs).

Lisa Chinyoka[1]

Abstract

Technology advancement comes with the burden of cybercrime, hence the need for cybersecurity and data protection. The objectives of the study were to determine if SMEs employ technical cybersecurity measures, to identify challenges faced in employing cybersecurity measures, and to establish if stakeholders are involved in policy making. The Routine Activities Theory was used to explain crime causation. The research methodology consists of a mixed methodology approach. Fifty (50) Small and Medium Enterprises (SMEs) were chosen as the study sample through stratified random sampling and purposive sampling. The Statistical Package for the Social Sciences (SPSS version.24) data analysis tool was used to analyze the quantitative data, and thematic analysis was used to analyze qualitative data. The findings reveal that most businesses do not implement some technical cybersecurity measures. Cybersecurity policies are not being formulated nor implemented. A lot of businesses do not conduct staff training on cybersecurity and data protection. Advancements in technology make it difficult to implement cybersecurity measures. It is recommended that organizations employ technical and human-centered cybersecurity measures. Businesses should invest in technical cybersecurity measures and use cybersecurity policies and legislative measures. The private sector should cooperate with the government.

Keywords: Technical measures, data protection; cybercrime, SMEs, cybersecurity

1. INTRODUCTION

The advancement in technology creates opportunities for business, seamless communications and leisure activities to thrive according to Eze et al (2022). According to Maphosa (2023), the internet is growing in volume and complexity and without proper handling criminals can access data and information. The number of cyber-attacks is increasing and daily rising according to a number of a studies (Zwilling, Klien, Lesjak, Wiechetek, Cetin, Basim (2022), Ponemon (2018) and Ukwandu et al (2022).This study is important because, as proposed by Ghauri (2021) governments, companies and financial institutions use information technology to handle private information and this information needs to be protected. The main aim of this study is to identify the challenges faced by Small and Medium Enterprises (SMEs) in implementing cybersecurity and data protection measures. The research objectives of the study are: to determine if SMEs are employing technical, cybersecurity measures, to identify the challenges faced in employing cybersecurity measures and to establish if stakeholders are involved in policy making.

2. RELATED WORK

Literature provides insights into the concepts of cybersecurity and data protection and privacy and how it operationalizes in the work environment. It provides a critical understanding of the benefits of cybersecurity and data protection in the workplace and how companies need it to protect their data and computer systems. The literature also looks at how organizations in African countries struggle to protect their systems due to various factors.

Hamburg and Grosch (2018:4) emphasize that the need to protect people and organizations from cyberattacks is very important. In order to avoid decisions which could negatively affect organization reputation, a comprehensive and strategic crisis communications plan is necessary according to Davies (2016). Incorrect decision making comes about when people are ill-informed about cybersecurity and data protection issues and act in ways that make them vulnerable to cybercrime. The plan should include basic key messages and categories of information the firm will need to share with its audiences in the case of an attack. The stakeholders to be involved include employees, customers, media relation department as well as C-level execs who hold the senior leadership positions within a company.

[1] Bindura University of Science Education, Department of Intelligence and Security Studies, 8797 Mangwende Highfield Harare

According to the International Telecommunication Union, 2020, “cybersecurity is a shared responsibility which requires coordinated action on the part of the government authorities, the private sector and the civil society”. Although the responsibility is shared, it is always the responsibility of organizations to make sure they are well protected. For this to operate smoothly and to ensure a safe, secure and resilient digital realm, a comprehensive framework or strategy is necessary which has to be developed, implemented and executed in a multi-stakeholder approach.

Stake holders who are directly or indirectly affected by the activities of the business are relevant when it comes to cybersecurity, because everyone has an interest in ensuring a free, open and secure cyberspace and these stakeholders may belong to a range of stakeholder groups including:

1) Different government departments
2) Public bodies such as telecommunications regulators
3) The judiciary and law enforcement
4) Civil society groups like those with expertise in human rights
5) International and regional organizations whose mandate or expertise includes cybersecurity
6) The technical community
7) The private sector particularly those from industries and sectors that are vulnerable to cyberthreats.

Akanle et al (2020) recommend a multi-stakeholder strategy for cybercrime in Nigeria that includes government agencies, commercial sector organisations, civil society groups and international partners.

Organizations can considerably lower the risks of cyberattacks and their associated expenses by implementing appropriate cybersecurity policies. A study conducted by Anderson et al (2021) found that companies that invested advanced security technologies, employee training and incident response plans experienced 95% fewer cyber incidents and saved an average of 1.5 million per year compared to those without adequate cybersecurity measures. “Policy” refersto information distribution rules and regulations, private sector goals for data conservation, system operations strategies for technology control according to Li and Liu (2021).

A business that emphasizes security, by involving employees and implementing clear procedures, creates an environment that tackles numerous underlying issues that would otherwise contribute to data breaches (Aslan et al, 2023).To establish effective organizational cybersecurity, senior employees must follow a four-step process: identifying the company’s critical assets, developing an understanding of relevant threats, designing procedures to prevent cybercrime and educating and engaging staff (Bada &Nurse, 2019)

The creation of cybersecurity standard guidelines have been identified as one of the factors influencing the development of an effective cybersecurity culture by researchers. The lack of a credible cybersecurity policy has caused many companies in many nations to fail to counter cyberattacks (Lippert and Cloutier, 2021).

Qualitative work to prevent cyberthreats is directly related to an effective system of human capital management. Whether the management can keep their employees motivated and focused on the result, how accurately the security relationship system is built, whether employees feel their involvement and responsibility for the quality of work done and are ready to follow the established rules of digital behavior directly depends on the degree of cyber sustainability of the company. Too many safety measures can cause staff psychological discomfort which can lead to dissatisfaction with work, reduce their level of involvement and responsibility for the quality of work done. Cultural practices such as open communication, responsibility and ethical leadership only lead to secure behaviour if employees are well involved to internalize and implement those values (Tran et al, 2025).

Cybersecurity awareness is a key driver of the extent to which employees are aware of, react to, and mitigate information security threats within organizations (Yogi & Aiswarya, 2025). Awareness of different sorts of cybercrime and their effects is important in moving in an increasingly digitized environment.(Hussein, 2024). As technological advancement progresses and change interactions across all aspects of society, it is vital to be aware of these threats to ensure the safety of lives online and offline

(EC-Council, 2024). Employees in organizations with a high security culture carry out proactive compliance behaviours even without direct supervision (Iyer & Raji, 2025). Participating in training initiatives promotes vigilance towards phishing and social engineering attacks and employees can make more frequent reports of suspicious behavior (Alauthman et al, 2025). Onyema et al, 2021 examined the role of cybersecurity awareness in mitigating cyber identity threats and found that cybersecurity awareness among users can significantly reduce the risk of identity theft and fraud

Connolly et al (2020) conducted a study on the experiences of organizations that have fallen victim to ransomware attacks. Using quantitative and qualitative data from fifty (50) organizations in the UK and North America, they assessed the severity of crypto-ransomware attacks .They found out that an organization's security posture influenced the severity of a ransomware attack. Organizations that have weak security postures suffer harsher outcomes of ransomware attacks as opposed to companies with stronger postures.

Network security is a specialized field in computer networking that involves securing a computer network infrastructure and is typically handled by a network administrator who implements the security policy, network software and hardware according to Veda and Sujatha (2019). They note that network security typically relies on layers of protection and consists of multiple components including networking monitoring and security software in addition to hardware and appliances.

Many organizations fail to prioritize application security leaving their entire environment at risk and it is prudent to adopt a risk based application security management according to Deloitte-Risk Advisory (2018). They further note that securing applications is a multi-faceted activity that needs thorough understanding of the application behavior and its various functionalities.

According to Takabi and GhasemiGol (2019) the Cloud is vulnerable to a variety of treats and attacks that affects the growth of cloud computing in recent years. Cloud security consists of different aspects such as infrastructure, information and identity.

Infrastructure security includes the physical assets that make internet connectivity possible. These include network devices such as routers, switches, firewalls, Intrusion detection systems, proxy servers and IXPs (Internet society and Africa Union, 2017). Various virtual, intangible or abstract components are also needed for the internet to function such as addressing, routing, application protocols and services and the Domain Name System (DNS).

Strong encryption is an essential element of our digitized democracies and helps to ensure protection of our most fundamental human rights and security of our digital economy however the utility and effectiveness of these technologies also facilitates significant opportunities for criminals according to Europol (2019). Microsoft (2020) identified emerging threats such as AI - enabled capabilities to commit cybercrime and increased adoption of IoT and teleworking.

Based on a study by Rabogadi (2019) in Botswana, the development of appropriate policies and strategies to fight cybercrime and protect national infrastructure assets is lacking. According to Ghauri (2021), cyber-risk measures and control of financial institutions should be as well as any other corporate risk and it is the duty of teams in the server room and a corporate strategy encompassing all employees.

Many African countries still use outdated or in many cases unlicensed, software according to Tahiru (2018). He further goes on to say that nearly one quarter of users in Africa are currently using the operating system, Microsoft Windows XP which was first released in 2001, and for which software patches were discontinued in 2014.This means that computer systems remain vulnerable to cyberattacks because cybercriminals are always coming up with new softwares. Cybersecurity measures require a huge investment, which may be beyond the reach of most of the retail businesses according to Mugari et al (2023). The emergence of cryptocurrencies, has perpetuated cybercrime due to their pseudonymisation and decentralized nature (Swiatkowska,2020). Due to limited resources, inadequate infrastructure and limited access to skilled cybersecurity professionals, developing countries often face challenges in implementing effective cybersecurity capacity building and commitments (ITU,2021).

As of January 2018, over 100 countries around the world have enacted comprehensive data protection legislation, and around 40 countries are in the process of enacting such laws (Privacy International (2018). They go on to say that a data protection framework may have its limitations but it does provide an important and fundamental starting point to ensure that strong regulatory and legal safeguards are implemented to protect personal data. These limitations are brought about by technological advancement including sophisticated profiling and tracking, artificial intelligence, means that some existing data protection laws are out of date and unfit to deal with processing as it currently functions.

According to ALT Advisory Africa (2020), in Zimbabwe the Cyber Security and Data Protection Bill was published in the Zimbabwean Government Gazette and is intended to consolidate cyber-related offences and provide for data protection. The Data Protection Act (Chapter 11:22), seeks to "create a technology driven business environment and encourage technological development and the lawful use of technology". The bill contains provisions on dealing with security and security breaches and encourages data controllers to put in place proper internal procedures and processes detecting, investigating and reporting data breeches amongst others according to `OneTrustDataGuidance (2023).Adaptation and alignment of legal frameworks are often time-consuming and difficult, due to the rapid evolution of the cybercrime threat landscape according to Europol (2019:14).

Strong encryption is an essential element of our digital democracies, and helps to ensure the protection of our most fundamental human rights and the security of societies. Nevertheless, the utility and effectiveness of these technologies also facilitates significant opportunities for criminals. EU law enforcement authorities indicate that a significant and increasing percentage of cybercrime investigations involve the use of some form of encryption to hide relevant data and communications evidence Europol (2019). This is a cross-cutting challenge that affects all crime areas, including cybercrime, serious organized crime and terrorism.

3. PROBLEM STATEMENT

Small businesses are essential to the economy and contribute significantly to job creation (Saha& Anwar, 2024). Attackers often target smaller firms assuming that these businesses may not be adequately prepared to handle a network security breach (Wolf et al, 2021). Businesses in developed countries are often most affected by the abuse of internet services to facilitate cybercrime and developing countries are equally at risk (United Nations Office on Drugs and Crime, 2020).The National Risk Assessment (NRA) report of 2020 recognizes cyber risks particularly through digital financial channels among other crimes as contributing to an estimated US 900 million dollars of illicit proceeds generated in Zimbabwe from criminal activities. According to a survey by Shepherd (2023), 60% of small businesses that experience a cyber-attack shut down their business within six months. SMEs in Zimbabwe face various challenges when it comes to fully implementing cybersecurity measures as they adopt different technologies (Mataruka et al, 2025).

4. CONCEPT AND TERMS

According to Hamburg and Grosch (2018:45), cybersecurity is a broad term which comprises the protection of critical information infrastructure from hackers as well as elements which are considered critical information infrastructures such as information networks of small to medium sized enterprises or personal computers. Benefits of cybersecurity include enhancing the company's work, improving customer happiness, reducing bureaucracy and enhancing cash flow, safety and certainty as proposed by Ghauri F, A (2021). The need to prevent these cyberattacks then puts forth the need for businesses to protect their systems. According to a Checkpoint press release (2020) a cyber-attack is an assault launched by cybercriminals utilizing one or more computer devices against a single or multiple computer devices or networks. Cybersecurity ensures data integrity and confidentiality by guarding against unauthorized access to sensitive information (Mukiibi, 2019). A report by Liquid Intelligent Technologies (Liquid)(2022) on three African countries South Africa, Kenya and Zambia identified email attacks, including spam, phishing and social engineering attacks as the most pressing cybersecurity threats. They also identified data breaches including data leakage, data disclosure and data extortion as being prevalent. Cybercriminals are misusing computers and utilizing techniques such as

denial of service attacks, network intrusion and distribution and supply of illicit data to commit acts of both criminal and undesirable behavior (Abdullah and Jahan (2020:219).

Data protection is commonly defined as the law which protects personal data. Data protection laws are aimed at protecting and safeguarding the processing of personal information (or personal data). This refers to any information relating to an identified or identifiable natural person that is the data subject (Media Defence, 2020:3). "Data protection is about safeguarding our fundamental right to privacy by regulating the processing of personal data that is providing the individual with rights over their data and setting up systems of accountability and clear obligations for those who control or undertake the processing of the data", (Privacy International (2018:12). Proper measures need to be implemented to protect personal data otherwise people end up losing vital information which may be very detrimental. Consumers hold the security of their personal data and other confidential information in high regard and the protection of user privacy and data is integral to the continuation of consumer confidence (Poremba, 2019).

Privacy International (2018:12) are of the view that privacy and data protection are intrinsically linked. Data privacy refers to the protection of personal information and data from unauthorized access, use, disclosure, disruption, modification or destruction (Mohsin, 2022). Data privacy involves things like ensuring that personal information is only collected and used for legitimate and authorized purposes, providing individuals with control over their personal data, and protecting personal information from bring accessed or disclosed without permission from the owner. (Mohsin, 2022).

Privacy is an internationally recognized human right according to Article 12 of the Universal Declaration of Human Rights (2015) which proclaims that , "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence….Everyone has the right to the protection of the law against such interference or attacks." Organizations need to ensure that privacy is maintained so that they do not find themselves at loggerheads with clients or employees. This is an aspect that requires attention and action to safeguard the rights of persons.

In this digital era, SMEs are becoming more dependent on digital technologies for their operations making cybersecurity a critical concern (Benjamin et al, 2024).Zawaideh et al, 2023) focus on cybersecurity threats in the context of e-commerce as a great number of SMEs are making use of it these days. A lot of people believe that large organizations are more vulnerable to cyberattacks than small businesses due to the size of their operations due but this is not particularly true (Saha& Anwar, 2024).

4.1. Theoratical underpinnings

Cohen and Felson developed the Routine Activities Theory theory (RAT) in 1970 which proposes that elements of a criminal or deviant act come together in normal, legal and routine activities according to Schaefer (2005). Cohen and Felson (1979) stated that there must be a motivated offender, a suitable target and the lack of a capable guardian. They articulate that when these three elements converge in time and space then crime occurs. This is to say that when the motivated offender comes in contact with the suitable target in the absence of a capable guardian, that could prevent the offender from committing crime then crime will occur. This theory resonates with this particular study because it explains the elements required for crime to occur and therefore puts into focus what to look out for in crime prevention. The motivated offender would be the cybercriminal, the suitable target would be the business' computer system and the capable guardian would be the system administrators of the SMEs. Cyberspace is a high crime rate place where offenders are always looking for a suitable target and the function of cyberspace creates opportunities for motivated offenders (Hasan, 2022) Cyberspace itself provides tools that make it easier for the offender to attack a target (Leukfeldt and Yar, 2016). The function of cyberspace creates opportunities for motivated offenders because physical distance does not matter between victim and offender.

5. SOLUTION APPROACH

The study was based on a mixed methods approach that is both quantitative and qualitative data was collected and analyzed. The variables also have both qualitative and quantitative research elements. The mixed method approach allowed for data triangulation as both qualitative and quantitative data was collected. The explanatory sequential type of mixed research was used and quantitative data was analyzed first and the qualitative data was analyzed next. Descriptive statistics were used to describe key features of the data. Quantitative data was analyzed using Statistical Package for the Social Sciences (SPSS version .24) and Excel whilst qualitative data was analyzed using thematic analysis .The study was carried out in the Harare Central Business District (CBD). The study was based on fifty (50) SMEs in different lines of business to get an all-round view. The businesses were categorized as financial services providers, pharmaceuticals and car spares and accessories. The population was 162 registered SMEs as provided on SMEAZ online directory (2025). To arrive at the sample size Yamane's online calculator was used and it is for calculating finite populations. The sample size was calculated as follows:

N/K+ N(e)^2

Where N=population of study

K=constant

e= degree of error expected

n=sample size

162/1+162(0.05)2 =115

Through stratified random sampling, the SMEs were grouped into the following categories: Financial Services Providers , Pharmaceuticals and Car spares and Accessories.The sample size specifically comprised of the following Financial Services Providers (15), Pharmaceuticals (20), car spares and accessories (15). The total sample size was 50.

Purposive sampling was used to select only respondents who had more information on the subject area. The data was collected from Information Technology (IT) staff, administrators and staff from Finance. An open-ended questionnaire was used to collect quantitative data during the survey and an interview guide was used to collect data from interviews. Both instruments were pre-tested first on a similar group and were found suitable for this study. The researcher however notes that generalizability of the study might be impossible due to the small sample size**.**

6. ANALYSIS OF RESULTS

6.1. Gender of respondents

The following table shows the gender of the respondents:

Table 1: Gender

	Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Male	35	70	70	70
Female	15	30	30	100
Total	50	100	100	

Table 1 shows that there were more males than females who were dealing with cybersecurity issues in the sector. This shows male domination in the computing sector and more females might need to be educated in the area of cybersecurity.

6.1.2. *Qualifications of respondents*

Table 2 shows the qualifications of the respondents:

Table 2: Qualifications

	Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**

Undergraduate	30	60	60	60
Masters	20	40	40	100
Total	50	100	100	

Source: Primary data

Most of the respondents had an undergraduate degree and three of them had a Masters Degree. This was attributed to the complexity of cybersecurity and hence businesses having to employ people with higher qualifications and who have the ability to handle computer systems.

6.2. Cybersecurity technical measures

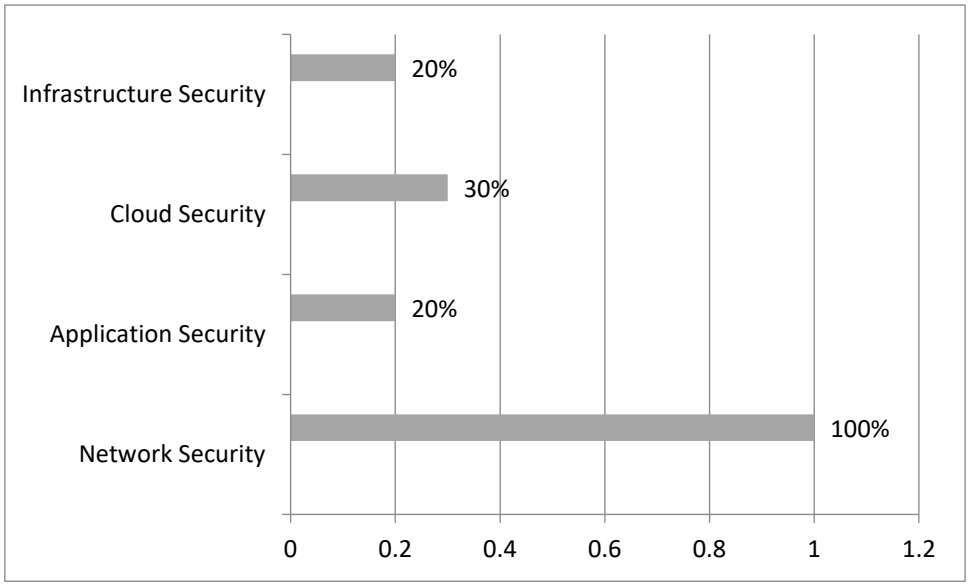

Fig 1: Cybersecurity technical measures

Source: Primary Data

All of the respondents use network security in their business as indicated by the results above. This could be due to the fact that it is commonly used and cheaper than other types of security. The results show that 20% of the respondents use application security in their business. This therefore means that their systems are vulnerable to cyberattacks. Only 30% of the respondents use cloud security in their business. This might be due to the expenses associated with the softwares needed for cloud security thereby making most firms unable to purchase them. Computer systems are therefore not fully protected from cybercrimes. All of the businesses indicated that they do not have infrastructure security. This also makes them easy targets for cyberattacks**.** Such exposure to cybercriminals puts small businesses at risk and the importance of protecting computer systems can never be overemphasized. This indicates that a lot of computer systems are vulnerable to cyberattacks as they are not being protected. Most of the technical measures of cybersecurity are not being implemented in Zimbabwe and this might be due to lack of funding to implement them and network security is being given more priority. The consequences of that will be vulnerabilities in computer systems exposing them to attacks .This is also alluded to by Mugari et al (2023) who are of the view that cybersecurity measures require a huge investment, which may be beyond the reach of most of the retail businesses. However SMEs might not have many financial resources as would bigger firms.

6.3. Cybersecurity Non-technical Measures

6.3.1. Availability of a cybersecurity policy at the organisation

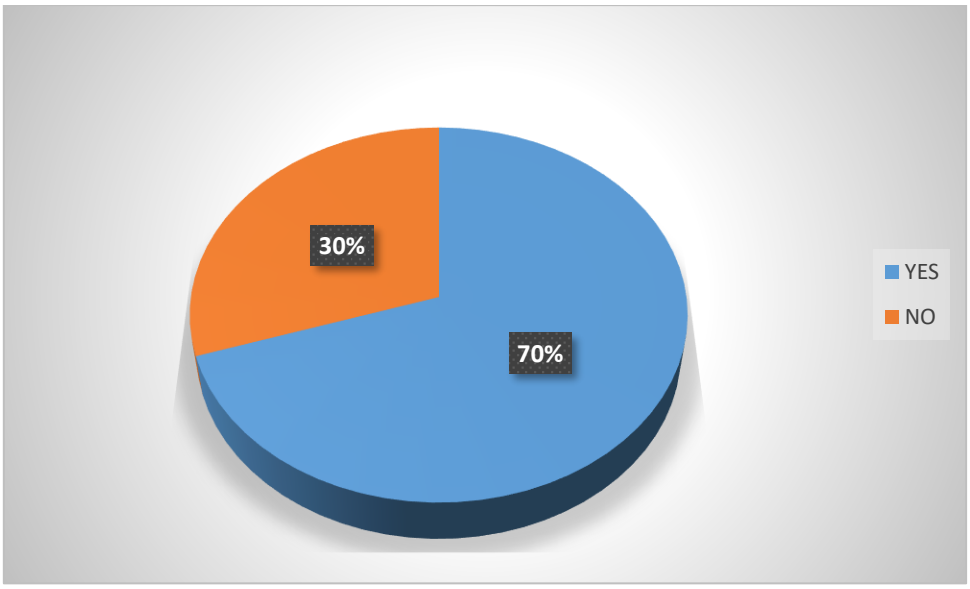

Fig 2: Availability of a cybersecurity policy at the organisation

Source: Primary data

Most of the respondents relayed that they do not have a cybersecurity policy at their organisation. A cybersecurity policy is important in protecting a company from cyberattacks as evidenced by (Lippert and Cloutier, 2021) who assert that the lack of a credible cybersecurity policy has caused many companies in many nations to fail to counter cyberattacks. A company has to formulate a cybersecurity policy that caters to its specific goals and environment without failure. Some businesses might lack the knowhow on how to go about it and others might be oblivious to its importance. A cybersecurity policy would equip employees with skills to respond better to cyberattacks. This is evidenced by the study conducted by Anderson et al (2021) who found that companies that invested in advanced security technologies, employee training and incident response plans experienced 95% fewer cyber incidents and saved an average of 1.5 million per year compared to those without adequate cybersecurity measures. This is also consistent with the study by Rabogadi (2019) in Botswana where they found out that the development of appropriate policies and strategies to fight cybercrime and protect national infrastructure assets is lacking. This also means that effectively combating cybercrime becomes difficult as procedures are important to establish effective organizational cybersecurity, senior employees must follow a four-step process: identifying the company's critical assets, developing an understanding of relevant threats, designing procedures to prevent cybercrime and educating and engaging staff (Bada &Nurse, 2019). SMEs do need to take the necessary steps in coming up with effective policies which will ensure that cybersecurity is enhanced. Cultural practices such as open communication, responsibility and ethical leadership only lead to secure behaviour if employees are well involved to internalize and implement those values (Tran et al, 2025) and with the absence of a clear cybersecurity policy these practices may never be fully implemented.

6.3.2. Involvement of stakeholders in policy formulation

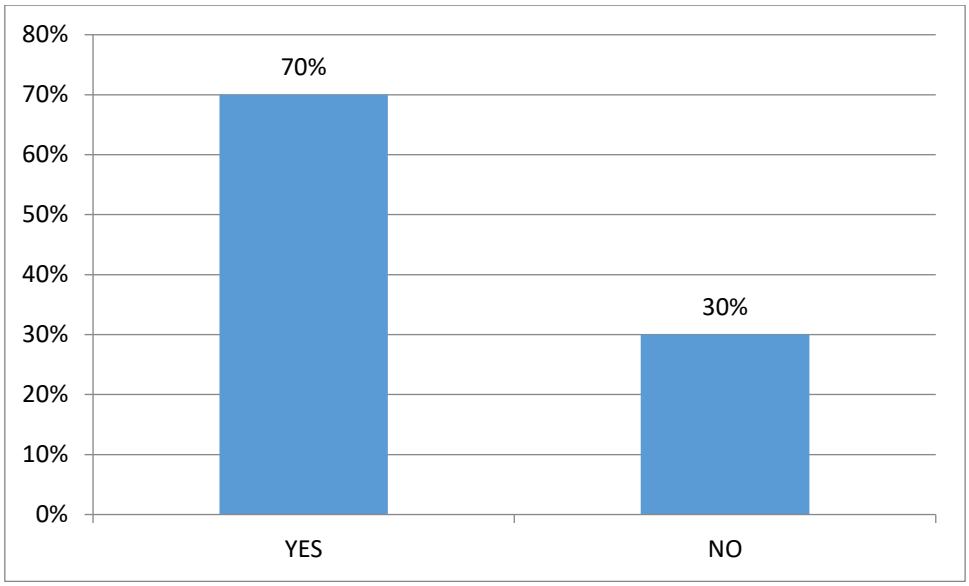

Fig 3: Involvement of stakeholders in policy formulation -

Source: Primary data

Most firms do not involve stakeholders in cybersecurity policy issues. This could be attributed to the lack of knowledge that stakeholders both internal and external should be involved in cybersecurity issues. This is supported by the International Telecommunication Union, 2020, that "cybersecurity is a shared responsibility which requires coordinated action on the part of the government authorities, the private sector and the civil society". This means policies could be drafted but implementation becomes almost impossible if other stakeholders are not on board. This also comes to show how the human element should always be considered when implementing cybersecurity measures as well. This is in line with the view by De Bruijn and Janssen (2017) that limited understanding and awareness of cybercrime and cybersecurity substantially exacerbate lack of planning and development of an appropriate policy framework to safeguard critical information assets. Involvement of stakeholders would make them more willing to accept the cybersecurity policy as well. In light of this SMEs need to know the needs of different stakeholders and how these can be addressed in the policy to get a better outcome.

6.3.3. Staff trainings on cybersecurity and data protection

The table below shows staff trainings on cybersecurity and data protection

Table 3: Staff trainings on cybersecurity and data protection

	Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Regularly	5	10	10	10
Occasionally	10	20	20	20
Never	35	70	70	100
Total	50	100	100	

Source: Primary Data

Staff trainings on cybersecurity are not being done regularly. The lack of staff training on cybersecurity will make the organization vulnerable to attacks from cybercriminals. This is consistent with the findings of Anderson et al (2021) who note that employee training combined with other strategies will help to reduce cybersecurity incidents. As suggested by the Routine Activities Theory, the absence of a capable guardian will make occurrence of cybercrime possible thus untrained staff are vulnerable. Employee training will put the employees in a better position to protect systems from cybercriminals and prevent losses to the organization. Therefore SMEs should come up with proper plans on training their staff as well as upgrading those skills over time as cybercriminals are always inventing new ways to commit crimes.

6.3.4. Funding for Cybersecurity and Data Protection

The table below shows funding for Cybersecurity and Data Protection:

Table 4: Funding for Cybersecurity and Data Protection

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	20	40	40	40
Total	50	100	100	

Source: Primary Data

The results show that most of the companies do not have funding for cybersecurity and data protection. The economic environment has been turbulent and most organizations might be focusing on other direct costs. Cybersecurity infrastructure is expensive to acquire leaving many companies without a choice but to operate with systems which are not secured or protected. This is also noted by Mugari et al (2023), who relay that cybersecurity measures require a huge investment not afforded by many businesses. Small businesses are mostly affected by lack of funding and may not be able to fully invest in cybersecurity.

6.3.5. *The effect of advancement in technology on Cybersecurity and Data Protection*.

The table below shows the effect of advancement in technology on Cybersecurity and Data Protection:

Table 5: The effect of advancement in technology on Cybersecurity and Data Protection.

	Frequency	Percent	Valid Percent	Cumulative Frequency
Yes	30	60	60	60
No	20	40	40	100
Total	50	100	100	

Source: Primary Data

Most of the respondents strongly agree that advancement in technology has made it difficult to implement the Cybersecurity and Data Protection measures in the Cybersecurity and Data Protection Act. Technology advancement is making cybercrime more sophisticated and difficult to curb. This hurdle has significant implications on organizations' ability to fight cybercrime. Microsoft (2020) identified emerging threats such as AI - enabled capabilities to commit cybercrime and increased adoption of IoT and teleworking as well.

Thematic analysis was used to analyze the qualitative data and it involves reading through a set of data and looking for patterns in the meaning of the data to find themes. The following themes were derived: Importance of a cybersecurity policy, adequacy of funding to implement Cybersecurity and Data Protection measures, advancement in technology and Cybersecurity and Data Protection measures in the Cybersecurity and Data Protection Act and strategies to improve implementation of Cybersecurity and Data Protection measures.

6.4. Importance of a Cybersecurity policy

Different views were highlighted by the interviewees. Some felt that stakeholders should be involved in the cybersecurity issues so that they are able to protect themselves as well as they are aware of the different measures used by the firm to protect itself and its stakeholders against cyberthreats. They were also of the view that the involvement of different stakeholders in policy issues allows for different views which help to come up with robust measures to protect the business from cybercrime. *"Stakeholders should always be involved in cybersecurity issues to allow them to feel like they are an important part of the organization especially employees and customers".* One respondent highlighted that issues to do with cybersecurity are sensitive therefore the fewer people who are involved the better.

6.4.1. Adequacy of funding to implement Cybersecurity and Data Protection measures

All five of the respondents were in agreement that there is inadequate funding to implement cybersecurity measures. This is because the software and hardware needed to protect computer systems

is expensive. Because of their small profits, most small businesses cannot afford to buy them or even hire a specialist to help protect their firms from cyberattacks.

6.4.2. Advancement in technology has made it difficult to implement Cybersecurity and Data Protection measures

All of the interviewees felt that advancement in technology has made it difficult to implement the cybersecurity and data protection measures because more software programs are being developed by cybercriminals and data breeches are on the increase. Another respondent felt that technologies like Artificial Intelligence are making cybercriminals to always be a step ahead of businesses.

6.4.3. Strategies to improve implementation of Cybersecurity and Data Protection measures

Most of respondents were of the view that adequate legislative measures should be put in place if Cybersecurity and Data Protection measures are to be implemented. They lamented on how Artificial Intelligence is now being used to commit cybercrime yet most do not have adequate knowledge on it and are also not adequately prepared to deal with it. Laws should be continuously reviewed to be effective against some of the new cybercrimes that are emerging. Law enforcement agents should be properly trained to deal with cybersecurity and data protection issues as it is difficult to get a cybercrime case solved in Zimbabwe. It is imperative also for firms to involve employees in creating cybersecurity strategies because they are vulnerable if they are not properly informed.

The view that a cybersecurity policy is important is shared amongst the majority of the interviewees. This might probably be because they do recognize its importance even though most are not implementing it. Absence of a cybersecurity expert or inability to hire one might hinder them from having a cybersecurity policy. With reference to the Routine Activities Theory, this means that there is lack of a capable guardian who can adequately protect computer systems and this creates an opportunity for cybercriminals to hack into systems. Most of the interviewees agreed that there is inadequate funding for cybersecurity measures and attributed it to the tough economic conditions. There is need for law enforcement to train its agents and capacitate them with the relevant skills to fight cybercrime so as to complement legislative efforts.

7. CONCLUSIONS

This study has revealed that SMEs are having challenges in implementing both technical and human cybersecurity measures. It has shed light on how vulnerable SMEs are to cybercrime and how they must improve on issues to do with cybersecurity in order to survive. Costs of acquiring the software to protect systems is expensive and beyond the reach of many MSMEs. Cybersecurity policies are not available for most of the SMEs and stakeholders are not made part of the cybersecurity and data protection issues in companies. Staff trainings on cybersecurity are not being conducted at most firms. This makes staff unaware of cyberattacks and how to avoid them. Advancement in technology has also made it difficult to implement cybersecurity and data protection measures for SMEs as AI makes it easier for criminals to come up with more sophisticated attacks.

Cybersecurity and data protection must involve both technical and human aspects. SMEs should try as much as possible to implement technical measures which will protect their systems and they should invest heavily in that. Cybersecurity policies should be implemented by every organization and employees and other stakeholders should be involved in cybersecurity issues. Regular staff trainings are important to make staff more competent in dealing with cyberattacks. Legislation should be reviewed regularly so that they are able to fully curb cybercrime. Lastly the fight against cybercrime should be inclusive of all stakeholders and the private sector should also make efforts to work with government.

8. FUTURE WORK

There is need for future research to dwell on other SMEs which are not in the Harare CBD alone but in other parts of the country as they may have other challenges which are particular to them. A bigger data

set would also assist in getting a bigger picture of the challenges and then coming up with better solutions on how to solve these.

9. ACKNOWLEDGEMENTS

I extend my sincere gratitude to my family and friends for their moral support during this research. I also wish to thank the participants who gave their valuable insights to make this research possible.

REFERENCES

Abdullah A. T. M, Jahan I (2020) Challenges of cyberpolicing in response of cybercrime to reduce victimization. International journal of research and innovation in social science. (IJRISS) Volume IV, Issue V, May 2020|ISSN 2454-6186

Akanle O, Richard S.B, (2020)*"Why has it been so difficult to counteract cybercrime in Nigeria*? Evidence from An Ethnographic Study. International Journal of Cybercriminology, vol 14, no 1,pp 29-43

ALT Zimbabwe gazettes Cyber Security and Data Protection Bill (2020) https://altadvisory.africa>2020/05/20

Alauthman, M., Al-Qerem, A.,Alateef S., Alomomani, A., Aldweesh, A (2025). Human-Centric Cybersecurity:Addressing Insider threats and organizational culture. In complexities and challenges for securing Digital Assets and Infrastructure (pp 435-456) IGI Global Scientific publishing. https://doiu.org/10.1007/s/10207-024-00918-9

Aslan O, Aktug S.S., Ozkan-Okay, M., Yilmaz A.A., Akin E, A comprehensive review of cybersecurity vulnerabilities, threats, attacks and solutions, (2023) Electronics 12(6) (2023) 1333, doi:10.3390/electronics12061333

Bada M., Nurse J.R.C (2019) Developing cybersecurity education and awareness programmes for small and medium sized enterprices (SMEs, Information, Computer Security 27(3)(2019)393-410, doi:10.1108/ICS-07-2018-0080

Benjamin L.B, Adegbola A.,E, Amajuoyi P, Adegbola M.D, Adeusi B.K (2024) Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies, Available from https://www.researchgate.net/publication/381001776 Digital transformation in SMEs identifying cybersecurity risks and developing effective mitigation strategies.

Checkpoint Press Release document. (2020) https://www.checkpoint-research-covid-19-pandemic-drives-criminal-and-political-cyberattacks-across-networks-cloud-mobile-hl-2020

Connolly L.Y., Wall D. S., Lang M., Oddson B (2020), Journal of Cybersecurity, Vol 6, Issue 1, 2020, tyaa023,https:doi.org/10.1093/cybsec tyaa023-2020

Davies J. (2016) Benefits of cloud communications in a crisis. http://www.business-cloudnews.cpm/2016/06/09/benefits -of-cloud-communications-in-a-crisis situation.

De Bruijn H., Janssen M. (2017) "Building cybersecurity awareness. The need for evidence-based framing strategies. Government Information Quarterly, 34 p.17. doi.10.1016/j.giq.2017.02.007

Deloitte Risk Advisory (2018) Network Security. https://www.deloitte.com

Ghauri F, A (2021), Why financial sectors must strengthen cybersecurity. https://sites.google.com/site/ijcsis. International Journal of Computer Science and Information Security (IJCSIS), Vol.19, No 7, July 2021

Eze O.J, Okpa T.J, Onyejegbu C.D, Ajah B.O (2022) Cybercrime: Victims' Shock Absorption Mechanisms. DOI:10.5772/intechopen.106818

Europol (2019) Internet Organized Crime Threat Assessment (2019) https://www.europol.europa.eu

Internet Society and Africa Union (2017) Internet Infrastructure Security Guidelines for Africa.https://www.internetsociety.org

International Telecommunication Union (ITU)(2021).Global Cybersecurity Index (GCI). Available at:https://www.itu.int/dms_pub/iyu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Hassan, Md. Nazmul, (2022)Applicability of Routine Activity Theory: An analysis based on cybercrime in Bangladesh.http://dx.doi.org/10.2139/ssrn.4265385

Hamburg I., Grosch K, R (2018) Aligning a Cybersecurity Strategy with Communication Management in Organizations. http://dx.doi.org/10.5772/intechopen.75952

Hussein J, A (2024) A comprehensive study of cybercrime and digital forensics through machine Learning and AI. Al-Rafidain. Journal of Engineering Sciences, Vol 3, Issue 1,2025.369-395.https://rjes.iq/index.php/rjes

Iyer, S.S., Raji, B. (2025). Cybersecurity Culture and Organizational Resilience: A Human-Centred Approach to Digital Risk Management. American Journal of Industrial and Business Management, 15(5), 748-766

Leukfeldt E.R, Yar M (2016). 'Applying Routine Activity Theory to Cybercrime: A theoretical and Empirical Analysis

Lippert K.J., Cloutier R., (2021) Cyberspace: A digital ecosystem, systems, 9 (2021) pp 48-6 https:doi.org/1080/01639625.2015.1012409

Liquid Technologies (2022)C2Cybersecurityreport.https://liquid.tech

Liu Q., Li Y. (2021) .A comprehensive review study of cyberattacks and cyber security: Emerging trends and recent developments. https://doi.org/10.1016/j.egyr.2021.08.16.126, Volume 7, pages 8176-8186.

Mataruka L.T, Mazarura J, Zishiri C., Garatsa C., Mugambiwa L.Z.,Jekese G (2025) Catalysing Digital Transformation for Small and Medium enterprises in Harare, Zimbabwe: A study of adoption drivers. Vol.03, No.04 (2025)265-280, doi:10.61552/jibi.aspur.rs

Maphosa V. (2023) An overview of cybersecurity in Zimbabwe's financial services sector. M DOI:10.126on88/F1000research.13215823.1

Media Defence (2020) Data privacy and data protection (Module 4) www.mediadefence.org.

Mohsin K., (2022) Data Privacy and Cybersecurity. SSRN eLibrary .https://papers.ssrn.com

Mugari I, Kunambura M, Obioha E, E , Gopo N, R(2023)Trends, impacts and responses to cybercrime in the Zimbabwean retail sector. Doi 10.1108/SC-03-2023-0011 Emerald Publishing Limited, ISSN 1757-8043

Mukiibi, H, (2019) Cybersecurity in Africa. The boring technology story that matters. DOI 10.114513368077

National Risk Assessment (NRA) (2020) https://zimra.co.zw. Retrieved on 22 January 2024

OneTrustDataGuidance.(2023) Zimbabwe: An overview of the Draft for the Cyber and Data Protection Regulations https://www.dataguidance.com

Onyema E., Deborah E.,Ugboaja.,S., Edmond, V., Agubosim, C.C., Richard-Nnabu , N (2021).Cybersecurity Awareness Among Undergraduate Students in Enugu Nigeria. 5, 34-42

Privacy International,2018,A guide for policy engagement on data protection.https://privacyinternational.org/data-protection-guide

Poremba, S, (2019) *The Cyber-risk Paradox: Benefits of New Technologies Bring Hidden Security Risks*, Security Boulevard, Boca Raton, FL, USA

Saha, B., Anwar Z (2024) A Review of Cybersecurity Challenges in Small Businesses: The imperative for a Future Governance Framework, Journal of Information Security, 15,24-39.https://doi.org/10.4236/jis.2024.151003

Shepherd, M, (2023), 30 Surprising Small Business Cyber Security Statistics. https://www.fundera.com/resources/small-business-cyber-security-statistics

Schaefer S. (2005) The Victim and His Criminal: A study of Functional Responsibility: Newyork: Random House.

SMEAZ ,Customer portal, (2025), https://www.smeaz.org.zw/shop-online

tps://www.smeaz.org.zw/shop-online

Swiatkowska J. (2020) "Tackling Cybercrime to Unleash Developing Countries'Digital Potential," Pathways For Prosperity Commission Background Paper Series,

Tahiru A, 2018, Cybersecurity in Africa: The threats and challenges. http://www.cyberpolitikjournal.org/

Takabi H., GhasemiGol M (2019) Introduction to the Cloud and Fundamental Security and Privacy Issues of the Cloud. https://doi.org/10.1002/9781119053385.ch1

Tran, D.V.,Nguyen , P.V, Le, L. F., Nguyen, S.T.N(2025) From awareness to behavior: Understanding cybersecurity compliance in Vietnam. International Journal of Organizational Analysis. 33(1), 209-229. https://doi.org/10.11081.IJOA-12-2023-4147

Ukwandu E., Ben Farah M.A, Hindy H., Bures M., Atkinson R, Tachtatzis, Andonovic I, Bellekens X (2022) .Cybersecurity challenges in the aviation industry .A review of current and future trends Information 2022 13(3):146

Universal Declaration of Human Rights (2015) udhr_booklet_en_web.pdf

United Nations office on Drugs and Crime (2020) World Drug Report. https://reliefweb.int>report>unodc

Veda V. Sujatha R. (2019) Network Security-Importance and types. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 15, 2019 (Special Issue) https://www.ripublication.com

Wolf, F., Aviv, A.J, Kuber, R. (2021) Security Obstacles and Motivations for Small Businesses from a CISO's Perspective. 30th USENIX Security Symposium (UNISEX Security 21),11-13 August 2021, 1199-1216

Yogi M. K, Aiswarya D. (2025) . Safeguarding Knowledge Assets: Exploring the nexus of human factors, organizational culture and social engineering in KM security . In Cybersecurity in knowledge management(pp.166-178) CRC Press

Zawaideh, F.H., Abu-Ulbeh, W., Mjlae, S.A., El-Ebiary, Y.A.B., Al Moaiad Y., Das, S.,(2023)BlockchainSolution for SMEs Cybersecurity Threats in E-commerce. International Conference on Computer Science and Emerging Technologies (CSET), Bangalore, India,https://dx.doi.org/10.1109/CSET58993.2023.10346628

Zwilling M., Klien G.,Lesjak D., Wiechetek L., Cetin F., Basim H.N., (2022) Cybersecurity awareness knowledge and behavior .A comparative study. Journal of Computer Information systems. 2022:62 (1):82-87 .https://doi.org/1080/08874417.2020.1712269