SMALL AND MEDIUM-SIZED BUSINESSES (SMB) IN OMAN DATA PROTECTION IN DIGITAL TRANSFORMATION POST-COVID-19 - GAP ANALYSIS AND RISK MITIGATION

by

Sukhwinder Singh

Student ID: 47976
Batch: August 2021

DISSERTATION

Presented to the Swiss School of Business and Management Geneva

In Partial Fulfillment

Of the Requirements

For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

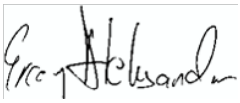
SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

<MONTH OF GRADUATION, YEAR>

SMALL AND MEDIUM-SIZED BUSINESSES (SMB) IN OMAN DATA PROTECTION IN DIGITAL TRANSFORMATION POST-COVID 19 - GAP ANALYSIS AND RISK MITIGATION.

by

Sukhwinder Singh

APPROVED BY 

.....

Dissertation chair

RECEIVED/APPROVED BY:

Renee Goldstein Osmic

Admissions Director

Dedication

I hereby declare that the work presented in the Thesis is entitled, “SMALL AND MEDIUM-SIZED BUSINESSES (SMB) IN OMAN DATA PROTECTION IN DIGITAL TRANSFORMATION POST-COVID-19 - GAP ANALYSIS AND RISK MITIGATION” in partial fulfillment of the requirement for the award of the degree Doctor of Business Administration and submitted to the Swiss School of Business and Management, Geneva is an original piece of work. The subject-matter discussed in the Thesis has not been submitted by me for the award of any other degree or in any other University.

Acknowledgements

Thesis writing is quite a tough task which requires support and mentoring from a lot of people inside and outside the academic world. In this regard, I would first like to thank my family members who have always been supporting me and kept on encouraging me in every task in the completion of this thesis.

Further, I would like to thank my advisor for his unwavering and invaluable support, guidance, and supervision at each step in order to complete this thesis. My advisor has supported me always and guided me with all the questions while clearing my doubts regarding the thesis process and in the statistical analysis as well. This helped me a lot in learning and developing my knowledge and experience throughout the dissertation as it was quite challenging for me at many stages of the thesis.

I would also like to extend my special thanks to the SBS University, Swiss School of Business and Management, Geneva for providing the necessary infrastructure and a great team of advisors, faculty members, and staffs for their continuous and unwavering support which offered a best learning environment for me and further allowing me to complete my study. Coming forward, I would also say a big thanks to my Academic Dean who has allowed me to attend the course and complete my study. Additionally, I would also thank the director of my Doctor of Business Administration as he has also been kind towards me and has also offered me with his unwavering support and guidance throughout my dissertation.

Finally, I would like to thank my friends who were always there by my side and kept on motivating me and making me laugh during the difficult phase of the thesis completion. Lastly, I'm truly thankful to God for these amazing people in my life who have supported me through the project completion.

ABSTRACT

SMALL AND MEDIUM-SIZED BUSINESSES (SMB) IN OMAN DATA PROTECTION IN DIGITAL TRANSFORMATION POST-COVID 19 - GAP ANALYSIS AND RISK MITIGATION

Sukhwinder Singh

2021

Dissertation Chair: Aleksandar Erceg, PhD

The main purpose of this research emphasises on exploring the data-protection and security concerns with the implementation of digital transformation within SMBs in Oman. The research objective focuses on determining the impact of data-related issues on the implementation of digital transformation, determining significant data-related challenges faced by management as a result of technical progress and inadequate security, and identifying recommendations to address the cybersecurity threats. Three hypotheses were formulated through extensive literature review to achieve the research objective.

Data were gathered by conducting surveys through close-ended questionnaires. The reliability of the questionnaires was performed using the pilot test by engaging 30 participants. Further, the survey involved 200 participants from the SMBs in Oman with at least 1 year of experience within SMBs who have adopted digital transformation within their business. The research has chosen a quantitative research methodology which has been analysed through statistical tests with the help of the SPSS software.

To test hypothesis 1, Pearson correlation has been performed between the digital transformation and data-related issues indicating a positive and robust relationship between the two. To test hypothesis 2, one-sample t-test, and one-way ANOVA have been performed to determine the challenges related to data indicating the p-value to be less than 0.05. The findings suggested that the management has been impacted with the data-related challenges because of technical progress and inadequate security. Lastly, the 3rd hypothesis aimed at determining the recommendations that assists in reducing the cybersecurity threats by performing the regression analysis. The results indicated a robust and positive relationship between the dependent and independent variable, further determining the p-value to be less than 0.05.

All the results from the study's hypothesis indicates a positive relationship between the adoption of digital transformation and data-related issues by determining the challenges along with the recommendations that help address the cybersecurity issues. wit

Table of Contents

LIST OF TABLES

List of Figures

CHAPTER I:

INTRODUCTION

1.1. Introduction

The dynamics of business has largely shifted towards digital transformation, especially after COVID-19 (Klein and Todesco, 2021). This shift has resulted in offering businesses with numerous benefits as well as challenges. Before COVID-19, the business world has been following the traditional method of operating businesses, however, the pandemic led to the adoption of these technologies largely (Wu et al., 2024). Small and medium-sized businesses (SMBs) in the Sultanate of Oman has also shifted towards digital transformation post COVID-19 which resulted in offering the SMBs with advantages as well as disadvantages. As the pandemic led to physical interaction and traditional model constraints, most of the SMBs in Oman shifted towards the adoption of digital technologies to sustain their business operations, engage with customers, and stay in market competition (Mishrif and Khan, 2023). The increased adoption of digital technologies within SMBs brought major changes in the business, particularly in the field of data management, and protection.

Increasing shift towards digital technologies have significant benefits, despite the advantages, data protection is one of the most concerning aspects of adopting this technology within SMBs (Coleman et al., 2016). The transition towards adopting digital platforms within SMBs not only increases the data volume but it also increases its sensitivity. SMBs by implementing digital technologies emphasise on storing financial data, customer information, and proprietary business intelligence electronically, which becomes an easy target for cyberattacks (Rawindaran, 2023). However, Omani SMBs adopt digital technologies within their business operations to increase customer engagement, and efficiency by contending with the increased risks of data breaches, and cyber threats (Alkhattali, 2025).

As the pandemic led to adoption of digital technologies in almost every sector and every business, the competition within businesses have also increased. Similarly, SMBs

in Oman have also focused on being competitive which in turn, leads to increased risks of data protection. Additionally, shifting towards digital transformation also results in issues such as customer data privacy, and security (Uvarova, 2021).

1.2 Background of research

The implementation of digital technologies has transformed businesses worldwide, and SMBs in Oman are not exception. Omani SMBs have largely adopted digital technologies that helped in being competitive while ensuring to increase the chances of facing risks associated with data management and protection (Alriyami and Ahmed, 2023). Omani SMBs have largely adopted digital technologies to increase their resilience, especially on online platforms, online communication tools, and cloud computing. This enables them to continue with their business operations effectively while expanding their reach, and enhancing their service delivery (Alog et al., 2025).Despite this, the sudden transition from traditional methods of operating business to digital methods led to the introduction of several vulnerabilities, particularly data protection. This swift shift towards digital technologies exposed major gaps in the existing frameworks adopted by the SMBs in their data protection (Moric et al., 2024). These gaps occurred as the data protection framework was designed for pre-pandemic era where adoption of digital technologies was not a necessity for businesses and they do not have to handle the issues of cybersecurity.

Adaptation of digital technologies within SMBs in Oman along with its other counterparts resulted in forcing the businesses to adapt to the new changes while leveraging the digital technologies, and maintaining the sustainability, and competitiveness of the businesses (Al Sheibani, 2020). Oman being a developed nation has been focusing on fostering and adopting digital transformation with an aim to diversify the economy of the nation while reducing the dependence on the export of oil.

In order to promote digital technologies within SMBs in Oman, the government has launched several significant initiatives that aids in supporting the growth of SMBs with an increased focus on establishing Small & Medium Enterprises Development Authority (SMEDA) and Oman Technology Fund. This change in digital transformation within SMBs has resulted in various issues associated with the protection of data. As the

utilisation of digital technologies has risen, it has resulted in increased growth of data generation, transmission, and storage (Al Jabri and Matriano, 2023). Despite significant benefits of utilising digital technologies within SMBs, several challenges within SMBs also occur resulting in lack of resources, infrastructure, and expertise that further results in ensuring the privacy, and security of the customer`s data (Chidukwani et al., 2022).

As the Omani government focused on the development of significant laws and policies to help prevent data protection, and management, especially the electronic transaction laws, and personal data protection laws, the government has still emphasised on evolving the regulatory frameworks in order to aid SMBs when they struggle to adhere to the existing policies, and regulations because of lack of resources, and limited expertise (Belwal et al., 2020). The commitment of the Omani government to supporting digital transformation in the context of SMBs has been instrumental in defining the post-COVID business environment. Entities like the Small & Medium Enterprises Development Authority (SMEDA) along with the Oman Technology Fund have not only offered funding but have opened up spaces for ideation as well. There are examples of such targeted programs as the Digital Readiness Assessment Tool provided by SMEDA and aimed at checking the technological readiness of SMBs. This tool includes a readiness index for cyber defence providing an additional layer of protection from cyber threats while implementing digitization (Alqassabi, 2020). The Oman Technology Fund, however, has targeted the incubation of domestic technology startups in the cybersecurity niche suitable to Omani SMB's requirements. For instance, a company that was funded by this initiative recently developed an encryption service that runs on a cloud-only for small business firms with constrained IT budgets. Such attempts are highly commendable as they indicate that the government holds cybersecurity as instrumental to the accomplishment of sustainable expansion in digital processes. However, there are a few limitations when it comes to equal distribution of these resources due to limited internet and technological savvy, especially in the rural areas where the majority of the SMBs are domiciled (Rahman et al., 2025).

1.3 Statement of Research Problem

In the modern business landscape, Information Technology (IT) has evolved as an important tool for all business sectors and thus SMBs are not an exception from utilising this. The tool not only empowers the businesses to run operations, streamline transactions, manage client relationship but also allows for enhancing resource allocation. Thus this indicates that in the modern business world, the rapid shift towards digital transformation has reshaped the operations of the business whether it is a large size business or small size business (Schwertner, 2017). But as this has been already discussed that the research is focusing on SMB sectors, thus in this emphasises on understanding the challenges that the SMBs in Oman has faced in digital adoption and thus protecting the data. In addition to this, this has been witnessed that there has been drastic changes in organisational operational in the post pandemic period. In the post pandemic period, business is seen to be more dependable on the digital technologies (Bahador and Ibrahim, 2021). Although the system has facilitated many operations within the organisation but this has raised the concern for data protection and cyber security.

Although with the digital adoption the SMBs in the Oman have remain themselves to be competitive and efficient, in this competitive business world. But transformation in business strategy has introduced significant risks related to data security, privacy, and regulatory compliance (Saeed et al., 2023). Many SMBs in Oman are facing challenges with lack of efficient infrastructure that protects cyber security and thus this shows a demand for expertise infrastructure. Improper infrastructure makes the system vulnerable to cyber threats.

But with overtime, dependency on digital infrastructure shows a pressing need for strengthen these systems in order to prevent data breaches. Also with time as organisations are increasing expanding their digital footprints, it is becoming easier for the hackers to conduct data breaches, thus pushing the organisations to expose to cyber threats, data breaches, and regulatory challenges (Kshetri, 2017). SMBs in Oman face unique challenges in their digital transformation journey. Many organizations struggle with cyber security readiness, compliance with global data protection regulations, and the adoption of secure digital platforms. As the SMBs are restricted within a limited financial

structure this limits them in investing lump sum amount on cyber security infrastructure and thus this makes them susceptible to cyber attacks data leaks, and operational disruptions (Heidt et al., 2019). In addition to this the increasing reliance on cloud computing, remote work technologies, and online transactions has further amplified these risks. Also, the increased risks do not allow attracting large pool of customers towards the SMB and thus lowering their ability to invest on data protection infrastructure.

Despite the significance of this topic, this has been found that there is a lack of research which has focused on the data protection challenges that is being faced by the Omani SMBs in the post pandemic period. But this has been found that there is a lack of research that has been conducted on the specific data protection challenges faced by Omani SMBs in their post-pandemic digital transformation journey. This has been found that the majority of the research has only focused on the specific data protection challenges faced by Omani SMBs in their post-pandemic digital transformation journey. Existing studies primarily address broader cyber security concerns without tailoring insights to the unique operational and regulatory environment of SMBs in Oman. There is also limited analysis of how international data protection frameworks, such as the General Data Protection Regulation (GDPR), influence local businesses and whether Omani regulations provide adequate safeguards for SMBs navigating digital risks.

In addition to this in the post pandemic period as there has been an increased reliance on cloud computing, remote work mode and online transactions and this has enhanced the data breaches (Habib et al., 2022). In the age of digital transformation with the nature of cyber security threats, there is a pressing need for tailored cyber security solutions and regulatory frameworks that will empower the SMBs in Oman in addressing the specific challenges that they will face in their operations. Thus this study aims to offer an in-depth analysis of digital vulnerabilities and thus with this understanding the study will also shed light into SMBs in Oman. Thus the findings the of study will empower the SMBs in the Oman with best practices for ensuring data security, regulatory compliance, and risk mitigation strategies in the evolving digital economy.

To set the scene of the type of threats that can be witnessed among SMBs today, one might look at the 2022 ransomware attack on a logistics company based in Muscat. It was attacked recently after the company had moved its operations to the cloud and had to compromise customer's payment details as well as the supply chain in the process. It was noted that this attack used outdated firewalls and weak passwords chosen by the employees, which is still prevalent in SMBs where they hardly invest in proper IT training and security programs. The financial effects observed were a decline in the firm's quarterly revenue by a margin of 40% and customer trust erosion – due to which the two companies are currently involved in a long litigation battle over data negligence claims. One more real-life example is a retail business in Salalah owned by a family where the firm suffered from phishing scams as it went through a change in focus, and adopted e-business. This is because there was no multi-factor authentication and also the employees were not taught about the imminent threats that surround cyber security. These examples underscore an obvious issue: new technologies increase operational productivity when integrated into businesses' fabric but their undertaking lacks security investments in proportion (Alharbi et al., 2021). The above incidences also bring out the latent sequence of events in a cyber-attack whereby technical shortcomings turn into brand and regulatory risks that put added pressure on the scarce capital base of the firms.

1.4. Research Objectives

In the present environment, effective use of various technologies may offer better assistance in managing various processes that aid in maintaining security in the organisation. Implementing digital transformation can increase the likelihood of chances for an organisation to incorporate cutting-edge tools such as Artificial Intelligence (AI), cloud-based systems, security measures, and others that help to minimise various difficulties in that organisation.Considering this, the aim of the study emphasises on understanding data protection in digital transformation in SMBs in Oman post COVID-19 while conducting a thorough gap analysis, and determining risk mitigation strategies. With this focus, several objectives of the study are as follows:

Analyse how the digital transformation has affected the organisation's data-related problems in small and medium-sized businesses.

As SMBs in the Sultanate of Oman emphasise on progressing towards advance digital transformations, this research helps to gain valuable insights from the employees and staffs from the SMEs regarding the implementation of digital technologies to examine where there exists a positive impact or a negative impact of digital transformation on the data-related issues within the SMBs. This objective would further aid in understanding the role of digital transformation when adopted within the business while understanding if it has resulted in offering opportunities to the business or resulted in facing challenges due to advance digital technologies. The digital transformation in Omani SMBs has brought about certain changes and risks regarding data in the Omani retail and logistics industries. On the positive side, by embracing advancements such as cloud computing and artificial intelligence in analysing data, businesses benefit from easy access to data and better predictions regarding market trends. We have seen that there are also restrictive structural features, with fluctuating internet connection and high costs of more sophisticated techniques. Also, the changes in moving organizations to the online environment during the pandemic intensified the focus on real-time data information, which put pressure on traditional solutions and made them fragmented. On the other hand, regarding the sources, the staff have mentioned that through upskilling, friendly analytics, and data tools it is easier for teams to utilize data for customer segmentation and operations flexibility. However, ongoing skills dearth and reluctance to transform the working environment into a data-oriented culture require culturally relevant training. While government and private initiatives for strengthening digital literacy and providing subsidies for technology are being established as enablers, innovation, and development are being complemented with the concern of cybersecurity(Moreira et al., 2025).

- To assess various data-related difficulties that the management is facing as a result of inadequate security and technical progress

Under this objective, the research aims to determine if the operations management within small and medium-sized businesses faces data-related difficulties that further

result in issues related to data. Some of these issues involve technical progress, and inadequate security. Determining the answer to this research objective significant helps in understanding the challenges faced by organisation when adopting digital technologies. Additionally, this also helps in understanding the possible issues that are mainly faced because of the implementation of digital technologies that cause issues in technical progress and lead to inadequate security of data. This further causes increased risks of data management and protection. For example, the use of cloud computing within SMBs in Oman has revolutionised the data management within organisations by offering cost-effective solutions, scalability, and flexibility that can effectively store large amounts of data, however, it also leads to issues such as data loss, corruption, interoperability, data privacy that leads to hinder the technical progress of the technology. Omani firms particularly SMBs have increased the use of digital tools while they have less robust security measures and uneven digital development. Though cloud solutions enhance data storage, their implementation is not centralized hence revealing many loopholes in society such as encryption deficiency, access control deficiency, and inadequate response mechanisms to different events that lead to customer and operational data breaches. Most of them are still in place in different sectors inclusive of manufacturing and they do not interconnect will new platforms thus, they slow up information flow and real-time data analytics. They also affect the ability to invest in higher levels of security defence, so the organization has to use old-school products such as mere antivirus or standard firewalls which do not combat these complex attacks. Employees also identify that they are not adequately trained regarding data security resulting in accidental breaches or mishandling of data. For instance, IoT incorporates unprecedented big data into logistics while it still does not have defined procedures for handling device threats, thus increasing risk (Kgakatsi et al., 2024).

- To make a better recommendation that assists in reducing the problems with cyber security in small to medium-sized businesses.

Cybersecurity has been one of the major issues that are faced by SMBs in Oman. With the rapid adoption of digital technologies, small organisations have emphasised on

integrating information technology to reach new markets and enhance their level of productivity and efficiency. Adopting digital technologies is not the only thing that businesses need to integrate, it also need to implement significant cybersecurity measures in order to protect and prevent their business, customers, and data from cyberattacks and threats. Thus, this objective focuses on identifying significant recommendations that can be helpful in reducing the issues that occurs due to cyber threats and security and help SMBs expand their business and reach in the market. To enhance cybersecurity readiness and preparedness of SMBs in Oman, recommendations must take into consideration factors such as lack of personnel skills and resources. A prioritized approach is to use large-scale, automated threat detection solutions based on AI to detect threats in real-time, which can help deal with IT teams that are understaffed. Implementing the zero-trust security model can reduce the possibility of the unauthorized use of IT systems, especially as industries experience extended levels of hybrid work post-pandemic. Engagement can be done with Oman's National Computer Emergency Readiness Team (CERT) for a better understanding of threats common in those regions and the frameworks established for handling such incidents. Also for raising internal cybersecurity specialists, it is possible to stimulate the acquisition of cybersecurity certifications among employees with the help of state programs. Another measure that SMBs can also employ is shared security service where various sectors provide a collaborative front to protect against phishing and ransomware. Integrating contracts for cybersecurity, especially when working with cloud services, guarantees the compliance of third parties with national legislation on the protection of personal data. Even for non-technical personnel of an organization, learning modules that are format-sized can help blow out human error-related risks such as poor password selection. Last but not least, approaching the problem of how to form an efficient online insurance system with rather low tariffs that will be backed up by the heads of the regulatory authorities will help to minimize financial losses in case of breaches. All these strategies are aimed at enhancing innovation while strengthening security to meet the Oman Vision 2040 objectives and ensure business trust in growth sectors (Chidukwani, Zander and Koutsakis, 2022).

1.5. Research Questions

Based on the study`s objective, the following research questions have been formulated:

RQ1. What is the impact of digital transformation on data-related problems within SMBs?

RQ2. What are the different problems faced by organisation`s management leading to inadequate security and technical progress?

RQ3. What are some of the recommendations that assists in minimizing cyber-security problems within SMBs?

1.6. Significance of Research

The study of data protection research within small and medium-sized businesses (SMBs) in Oman, especially with a focus on digital transformation after COVID-19 emphasises on addressing critical gaps in the practices adopted for the protection of data while determining significant actionable strategies to mitigate the risks. With increasing shift towards digital technologies, especially during the pandemic, SMBs in Oman has largely adopted novel digital technologies, and platforms that aid in remaining competitive and operational (Bhat et al., 2024). Adopting this technology has become important for businesses to continue their operations while identifying the risks, and vulnerabilities associated with data protection (wang et al., 2024). Thus, conducting this research is significant to understand the dynamics of implementing and adopting digital technologies in Omani SMBs while addressing the challenges associated with its adoption.

Protection of data is the most important aspect of building trust, and integrity within the business (Syed et al., 2023). Similarly, preserving the confidence, and loyalty of customers is also important for Omani SMBs by ensuring the confidentiality, and security of gathered customer data by complying with the law. However, issues such as data breaches or cyberattacks can result in serious consequences that lead to monetary loss, legal issues, and harming business reputation (Wang et al., 2019). This helps in determining gaps in the current practices of data protection and further aid in providing

significant recommendations so that the research can focus on improving data protection frameworks within SMBs while ensuring to safeguard the interests of business and maintaining customer`s confidence.

Further, conducting the study is also considered significant as it effectively addresses the needs of SMBs to adapt significant strategies for the protection of data when implementing digital technologies. This further resulted in outpacing the development of adequate measures for the protection of data leaving businesses with increased risks of cyber security threats. Thus, by researching on this context, the difficulties due to data protection such as lack of compliance with regulatory frameworks, inadequate security measures, and insufficient risk management practices faced by Omani SMBs have been highlighted which further help businesses to understand their improvement area and can implement them by addressing the issues.

In addition, conducting the research determines findings that aid in adding a wider range of information on data security associated with data transformation. As there exists a large number of studies focusing on data protection in large companies, a notable gap has been identified in understanding how SMBs have emerged in developing nations like Oman while addressing the issues of data protection (Matriano, 2022). Focusing on this specific aspect, this study emphasises on offering valuable insights that are also relevant to similar businesses that effectively help in understanding the intersection of digital protection and transformation within Omani SMBs.

Conducting this study is also significant as it provides recommendations that are relevant based on the research context. By determining the challenges, the recommendations emphasised on offering solutions to address the determined issues by tailoring the specific needs of the SMBs for the implementation of effective data protection measures (Cahyono et al., 2025). This also aids in shaping the business landscape by determining the need for updated policies, and regulations to evolve the need of data protection while supporting the businesses and contributing towards the development of effective regulatory environments. The research holds great importance in managing contextual threats more common among Oman’s SMBs, namely socio-

economic dependence on the informal networks and cultural apprehensiveness about data openness. As a consequence of that acceleration, an unfortunate event of digital vulnerability attack and lack of adequate IT governance in SMBs has made it necessary to evolve frameworks compatible with Oman's tribal business ethos which is trust-centric rather than system-imbedded. The study also demonstrates how most integrations with supply chains from other countries, which are widespread among Omani businesses, increase the likelihood of issues such as cross-border inconsistency in data compliance. Thus, the identified threats (e.g. regarding handling personal data of tourists by SMEs operating in the tourism sector) can inform the development of sector-specific guidelines rather than offering blanket solutions. In addition, the study establishes the chain of events that occur in SMB-oriented economies where one breach affects multiple interconnected micro-markets.

1.7. Definition of Terms

Digital transformation: This refers to the process of utilising digital technologies within businesses to meet the changing needs of the business by understanding the requirements of the market, and industry (Kraus et al., 2021). Implementing advanced technologies help in the creation of new products, or modify the existing ones by understanding the business processes digitally. This involves transforming the operational efficiency, business model by changing the way of delivering products, and services, emphasising on specific business areas, and fostering technological culture (vial, 2021).

Data protection: It is defined as a practice that safeguards the sensitive information of the customers from corruption, unauthorised access, loss by ensuring the availability of data and by complying with the regulations (Nallakaruppan et al., 2025). This emphasises on encompassing measures that aids prevent data such as personal health information, financial data, and personally identifiable information. This can be done by considering principles based on data minimisation, accuracy, fairness, transparency, lawfulness, accountability, integrity, and confidentiality to secure and protect the data accurately.

Cyber threats: Cyber threats are malicious acts that leads to damage, steal, or disrupt important data or digital information which can occur due to data breaches, computer

viruses, Denial of Service attacks, and several other attacks (Aslan et al., 2023). These can also occur when there is a possibility of cyberattacks because of unauthorised access, disrupted or damaged information, stealing information, computer network, or other sensitive information. These threats mainly come from hostile nation-states, organised crime organisations, hackers, trusted users, or from unknown parties from remote locations (Ulsch, 2014).

Risk assessment: The risk assessment procedure focuses on identifying, evaluating, and analysing the potential threats and vulnerabilities that can harm the data and organisational systems further requiring proactive measures that can aid in mitigating the risks while safeguarding the sensitive information (Taubenberger, 2014). The risk assessment procedure involves identifying the assets, and threats by evaluating and prioritising the determined risks. Further, risk mitigation strategies are developed to implement policies, procedures, and security control by regularly reviewing, and updating the security measures to address the cyber threats (Eltaeib et al., 2024).

Small & medium-sized businesses (SMBs): SMBs are businesses that focuses largely on revenues, assets, or workforce below the threshold (Piza et al., 2016). Omani SMBs play a significant role in within the economy by employing large workforce, and shaping innovation. SMBs further incorporate digital transformation by identifying clear goals, prioritising initiatives, investment in training, and leveraging new technologies strategically. This further aids in adapting to change by monitoring the progress, and embracing flexibility by adapting the strategies effectively.

General Data Protection Regulations (GDPR): GDPR mainly emphasises on European Union regulation that is based on data protection, and information privacy that focuses on improving individual`s control based on the individual`s personal data while simplifying regulations for businesses (Hoofnagle et al., 2019). This policy strengthens data protection rights by complying with the data protection principles by specific organisations.

1.8. Scope of the Research

The scope of the study focuses on determining the gap analysis and risk mitigation strategies with the implementation of data protection in data transformation, especially in SMBs in Oman after COVID-19. The study initially emphasises on understanding the impact of digital transformation on data-related issues within SMBs in Oman. As businesses have emphasised on adopting data protection, it results in offering a large number of benefits to them. This is so because data protection is considered as a key component that enhances the strategic security of the business to manage the loss of data (Mokalled et al., 2017). Further, the impact of digital transformation on data-related issues is also a broad area worldwide, and Oman is not an exception that focuses largely on responding towards improved security for possible consumer data by aligning with significant policies, and legislations. Additionally, the research emphasises on maintaining a wider range ethics, and security by complying with the standards of the SMBs. This requires increased attention on the loss of data protection. Thus, the research emphasised on examining the impact of digital transformation within SMBs in Oman with increased focus on data security, and protection.

The research further focused on determining the problems faced by the management of the organisation that leads to inadequate security, and technical progress. Despite various benefits of adopting digital transformation, the study emphasised on understanding the challenges that the SMBs in Oman faces within their business management related to issues leading to technical progress, inadequate security, lack of compliance with regulatory frameworks, and insufficient risk management practices (Al Maskari et al., 2019).

Lastly, the study emphasised on identifying the recommendations that help in reducing the issues of cyber threats within SMBs. By proposing significant strategies, and recommendations with a focus on reducing the cyber threat issues faced by the organisations by aligning with the regulatory frameworks of Oman. This offers significant solution that tailors the specific needs, and constraints of the business by considering significant factors like industry-specific issues, resource limitations, and regulatory compliance requirements (Shandilya et al., 2024). By understanding this, the

study would contribute towards understanding effective measures for the implementation of data protection measures within SMBs in Oman without pressurising their operational capacities. Additionally, relevant recommendations based on the research context also focuses on shaping the landscape of the business by determining the increased need of updated policies, and regulations that aids in addressing the needs of data protection, especially in SMBs. This further contributes to the development of effective policies, and frameworks for the protection of data that supports SMBs in a better way (Bada and Nurse, 2019). The development of these policies help understand the gaps in the current regulations that contributes to create an adaptive and robust regulatory environment while determining the solutions to the challenges faced by SMBs. Additionally, the recommendations also focused upon equipping the stakeholders with valuable insights that supports the business in a better way to implement data protection strategies by understanding the situation of Omani SMBs in protecting data, and determining the areas for improvement to strengthen the data protection practices so that the SMBs can enhance their ability to recover from the issues of cyber threats.

1.9. Structure of the Research

The structure of the research has mainly involved six core chapters that are designed systematically in order to answer the research problems, objectives, and questions while understanding the scope of conducting the research. The structure further focuses on involving the method utilised to conduct the study by understanding the appropriate design, data collection, and analysis method. A detailed structure of the research is discussed below.

Chapter 1 – Introduction

The introduction chapter involves discussions of the background, and rationale of the study highlighting the gap regarding the implementation of digital technologies with a focus on the protection and security of data within SMBs, especially within Oman. This chapter further establishes the goal and objective of conducting this research that involve evaluating the impact of digital technologies within the small and medium-sized organisations. Further, it also focused on understanding the significant challenges faced

by the organisation and the recommendations that can be considered to protect against cyber security issues. This chapter further involves discussing the purpose, significance, and scope of the study. Additionally, this chapter also involves the research questions and the definition of important terms used in this study.

Chapter 2 – Literature Review

This chapter starts with the overview discussing the introduction and main purpose of the chapter, designing the conceptual framework by understanding and aligning with the prior theoretical underpinnings that help conduct the research in a structured manner. It then discusses relevant theories that aligns with the context of the research. Further the chapter involves explaining the existing studies by ensuring to align the studies` objectives with the present objectives. This helps to gain an in-depth understanding of the research objectives that helps determine the significant impact of implementing digital transformations within Omani SMBs, assessing challenges within organisation management due to the adoption of digital technologies, and identifying recommendations to protect against cyber security.

Further, the literature review chapter also emphasises on identifying critical gaps in understanding the management and protection of data with the implementation of digital transformations in SMBs in the strategic Omani context. These gaps further help in informing the development of the conceptual framework along with the hypothesis by ensuring to align them with the research questions. Finally, the chapter comes to an end by summarising the key insights from the literature review chapter with a focus on literature gaps, and explaining how the research further aims to address these gaps by conducting an appropriate research method.

Chapter 3 – Research Methodology

The research methodology chapter encompasses all the detailed information about the methods and procedures required to conduct the study. To conduct the research, the methods involve discussing the research design, approach, philosophy, method, survey-based strategy, questionnaire design, sampling approach, data collection methods, and data analysis methods that are used to conduct the quantitative study. The chapter further

involves the survey administration process that mainly involves professionals from SMEs in Oman along with this the ethical considerations underlying the research method has also been discussed in detail.

Chapter 4 – Results and Findings

This chapter Results and Findings emphasises on determining the answers to the research questions by comprehensively presenting the results of the survey questionnaire by gathering the responses from the respondents and analysing them through the statistical tool, SPSS. This allows to understand the findings of the research questions by clearly determining the impact of digital transformation, data-related issues, and the recommendations that can aid in protecting against cyberattacks.

Chapter 5 – Discussion

Chapter 5 involves the discussion of the findings that are determined through the statistical analysis. The chapter gives a detailed knowledge and understanding of the results and help understand the findings in a better and coherent way. Further, the chapter also focuses on comparing the results of the primary data gathered through survey to the secondary data in form of literature review.

Chapter 6 – Conclusion, and Implications for Future Research

The research finally comes to an end by this chapter where the study is concluded by revisiting the research questions and by summarizing how these research questions have been addressed through the outcomes by conducting appropriate research methods. Further, the chapter also discusses the theoretical, and practical implications along with the limitations and recommendations that are important for building research in the future.

1.10. Summary of the Chapter

This chapter of the research gives a brief introduction of the significance and background of the topic. As this has been highlighted that the research is conducted on the topic *"Small And Medium-Sized Businesses (SMB) In Oman Data Protection In Digital Transformation Post-Covid 19 - Gap Analysis And Risk Mitigation".* The rapid adoption of digital technologies by small and medium-sized businesses (SMBs) in Oman

has created both opportunities and challenges. With the digital transformation it has helped the businesses to be remaining competitive and efficient, but on the other hand, this has imposed risks The increased reliance on cloud computing, online platforms, and digital communication tools has amplified the vulnerabilities, thus forcing the SMB along with the customer to expose to cyber threats. Although the government of Omar has made contributions in supporting SMBs in their digital transition through initiatives such as the Small & Medium Enterprises Development Authority (SMEDA) and the Oman Technology Fund. But despite these initiatives of the government, many SMBs in Oman struggle with inadequate cyber security infrastructure, expertise, and regulatory compliance. Many SMBs in Oman lack the necessary infrastructure to safeguard their data, making them vulnerable to cyberattacks. Also financial constraints restrict them from investing in advanced cyber security measures. The increasing use of cloud computing, remote work technologies, and online transactions has further heightened these vulnerabilities, limiting SMBs' ability to attract and retain customers. Despite the increased concern for data security, and the significance of the topic, this has been noticed that there are few studies which and also the studies has only focused on the cyber security concerns without addressing SMB-specific operational and regulatory environments. Thus by conducting this research the researcher aims to bridge the gap and the study will emphasise on understanding the impact of digital transformation on data-related problems within SMBs, further the study emphasises on the different problems faced by organisation`s management leading to inadequate security and technical progress and lastly on the basis of findings of the study, the research made recommendations that will assists in minimizing cyber-security problems within SMBs.

CHAPTER II:

REVIEW OF LITERATURE

2.1 Introduction of the Chapter

This chapter aims to offer a comprehensive understanding of the academic literature that are considered relevant to investigate the rapid shift towards digital transformation leading to data protection within SMBs, especially in the context of the Sultanate of Oman. The chapter establishes the theoretical foundations through diverse research and focuses on synthesizing key themes in the existing studies to understand the research approach effectively. The chapter starts by discussing the most relevant theories of GDPR and PII that ground the phenomenon of examining the management, and protection of data with the adoption of digital transformation in SMBs. These aids critique the applicability of the research in guiding toward the research question, and hypotheses. The literature review chapter further explores different variables by aligning with the research objectives and questions as mentioned in Chapter 1. The chapter discusses existing studies by determining the impact of digital transformation on data-related issues within SMBs; understanding issues associated with data as a result of inadequate security, and technical progress; and exploring significant recommendations that help in reducing the issues related to cybersecurity within SMBs.

The literature review chapter also identifies significant literature gaps in understanding the current knowledge that centers mainly on the deployment of digital transformation due to which problems related to data management and protection occurs, especially in the small and medium-sized businesses (SMBs) in the strategic context of Oman. As the literature gaps are identified, now the chapter further emphasizes on the development of the conceptual framework by mapping the hypothesized relationships between the variables related to the shift toward digital transformation and the data-related issues that occur due to this implementation. Further, testable, and focused research hypotheses are then proposed based on the conceptual and theoretical framework and by aligning with the research questions.

At last, the chapter emphasizes on summarizing the key insights from the comprehensive literature exploring the context of the research in detail by briefly talking about the identified literature gaps and by delineating to address these knowledge gaps by

conducting the research further through an informed research methodology in the next chapter.

2.2. Theoretical background

2.2.1. Underpinning theories

Different businesses face different types of issues within their internal, and external operations among which data protection and management is one of the issues that occurs largely within organisations that have shifted towards digital technologies. The challenges of data management and protection mainly occur in a dynamically evolving digital age and can be successfully addressed by gaining a competitive advantage in the business. However, failing to do so can result in negatively affecting the business. Various research studies have been conducted earlier that have focused largely on understanding the different aspects of digital transformation within SMBs. While exploring this, a large number of studies have also emphasized on the protection, and management of data with the implementation of digital transformation that plays a crucial role in highlighting a clear picture of the digital technology used within the business.

The theoretical knowledge offers an invaluable contribution to the research by identifying some of the most significant theoretical lenses along with the theories that have been placed by aligning with the research context. The theoretical lenses firstly align with the impact of digital transformation on the data-related issues within the SMBs. Secondly, it aligns with the issues faced by the organisation management due to inadequate security and technical progress. And thirdly, the theoretical framework also aligns by assisting in the reduction of cybersecurity threats within SMBs. Involving academic theory further offers a significant conceptual framework to guide the research in these specific areas.

The research considers the contribution made by Davis through his Technology Acceptance Model Framework which is also called the TAM framework. This theoretical model mainly focuses on acknowledging and comprehending the main factors that allow

the organization to accept new digital technologies easily and using them for increased growth of the business.

In addition to this, the Risk Management Framework developed by the National Institute of Standards and Technology has also been considered in the research which emphasizes on involving a process that aids in the integration of privacy, security, and cyber supply chain risk management activities into the lifecycle development of the system. This approach focuses on controlling the selection and specification of the technology by considering the efficiency, effectiveness, and issues that occur due to the system.

Contrary to the Risk Management Theory, the General Data Protection Regulations Framework, also known as the GDPR focuses on safeguarding the personal data and privacy of the information provided by customers for making transactions that occur within the businesses. Additionally, as the framework sets guidelines to collect and process personal information for the individuals living in and outside of the EU so that they can have increased control over their data along with the organisation responsible for handling the sensitive data.

By aligning with the research questions, these theoretical frameworks provide an exceptional understanding for the protection and management of data by rapidly adopting digital transformations within SMBs, especially in the Sultanate of Oman. However, these result in quite a complex scenario of how these data can be protected when utilized in the professional world of SMBs.

The Technological Acceptance Model Framework developed by Davis discusses the acceptance of the information systems by offering a more user-centric perspective and constrained that predicts and explains end-user acceptance of novel digital technologies by understanding the use and ease of use of the newly adopted technologies. Davis in his TAM model clearly explained that the implementation of digital technologies within organisations is determined directly by the perceived usefulness that the organization experiences. This explains the extent to which the organization believes that the utilization of the digital technology results in better performance and productivity along

with perceived ease of use highlighting the technology usage to be free of effort. However, external factors including the interface design, documentation, and training affect the perceptions, considering the model to be extensively used for a user-level adoption studies across technologies. As stated by Nurqamarani, Sogiarto, and Nurlaeli (2021) the Technology Acceptance Model (TAM) provides behavioral insight as to why SMBs opt to support privacy-enhancing technologies. The awareness level of using data security tools also depends on the degree of usefulness which is also augmented by how easy they are to operate with the above model. Many firms small or medium-sized size will not invest in some cyber solutions whenever those solutions appear to be complex and will cost a lot of resources. The approach of training combined with user-friendly technologies can enhance adoption rates thus making it crucial to create appropriate cybersecurity education programs specifically for Omani SMBs.

The TAM model explains the process that enables the users to accept and utilise the new technology. The study explains that the model emphasizes on suggesting when the users are provided with the technology and what factors are responsible for influencing them to use the technology and how they will use it (Silva, 2015). The utilisation of TAM model to understand the management of personal health records which were mainly influenced by three factors perceived usefulness, perceived ease of use, and security towards intention to use. It further determined negatively moderated usefulness and intention to use (Alsyouf et al., 2023). The TAM model is utilized in peer-to-peer lending in Central Java to understand the impact on data security and privacy. Based on the social phenomenon, the study revealed that the perceived usefulness of the TAM model depends on the better data security and privacy of borrowers through the P2P lending platform. Additionally, this also indicated a significant influence on the perceived usefulness as the technology becomes easier to use (Putri et al., 2023).

As discussed by Balzano, Marzi and Turzo (2024). The Institutional Theory enables an understanding of the ways external forces affect SMBs' handling of data privacy issues. Organizations adapt their functioning as they interact with three external forces, namely, the coercive forces, the regulatory forces and the normative forces and

mimetic pressures. Companies need to implement data protection measures because the legal frameworks consist of governmental regulations and industry norms. On the other hand, as stated by Özbek et al. (2022) Normative factors include the acceptance of professional associations and commonly followed cybersecurity norms by expert practitioners putting pressure on SMBs to adapt and change their security behaviors. Businesses follow mimetic pressures by duplicating data privacy strategies that are implemented by other organizations that demonstrate positive outcomes. SMEs in Oman have now considered the compliance of their data privacy policies with international protocols as the key factor in their efforts to establish their credibility and competitiveness in the market.

In addition to the above discussed points Wirtz and Lwin (2009) explained that The Regulatory Focus Theory (RFT) describes organizational and individual motivation between prevention and promotion orientations. Small and medium businesses with a prevention focus on data privacy ensure compliance with the Personal Data Protection Law (PDPL) of Oman to stay clear of penalties. Businesses that comprise a promotion focus approach data privacy through strategic investments because data protection allows them to improve both customer trust and their market reputation beyond regulatory compliance. The willingness of Omani SMBs to fulfill basic legal requirements differs from their commitment to establish advanced cybersecurity strategies.

The NIST emphasized on developing the Risk Management framework as an important framework for organisations with a focus on setting up guidelines to identify, eliminate, and minimize risks. By developing this framework, the NIST helped in protecting and preventing the information system of the US government. Federal agencies under the NIST designed this framework so that businesses can easily adopt this, especially in the private sector. The implementation of digital technologies within businesses results in posing threats and risks related to data including IT issues, loss of capital, and litigation which is not easy to eliminate, especially in a running business. However, this framework helps businesses in minimizing these risks.

Data privacy in Omani small and medium-sized businesses (SMBs) can also be examined through supplementary conceptual frameworks in addition to the theories previously discussed. The Protection Motivation Theory (PMT) serves as a framework for understanding how entities adopt protective solutions after identifying threats. Small and medium-sized businesses in Oman follow PMT because their owners and employees first evaluate the intensity of cybersecurity dangers and their level of exposure to threats along with examining the effectiveness of protective actions before implementing any measures. Due to poor cybersecurity understanding many small and midsized businesses fail to recognize the seriousness of data breach threats. Data privacy measure implementation motivation strengthens because regulatory laws become stricter and businesses encounter increasing customer requirements regarding data security(Haag, Siponen and Liu, 2021).

The main components that are effective in minimizing the risks through this framework involve identification, measurement and assessment, mitigation, reporting and monitoring, and governance. The process of identification involves identifying the privacy, strategic, operational, and legal risks faced by the organization. In this process, the risk assessment is performed periodically as the business tends to change over time. The next process is measurement and assessment where a risk profile is created for every determined risk. After the risk profile is created, the measurement and assessment process start by measuring the risks based on capital, or by quantifying the cost of a security breach with the implementation cost of a security mechanism. The next step involves mitigation where the examination of risks is conducted which further determines which risks should be eliminated. For example, when an organization identifies increased risks of cybersecurity resulting in data issues, by incorporating risk management framework, the business integrates security controls to minimize these risks. The next component involves reporting and monitoring where the identified and minimized risks are reexamined and monitored carefully to ensure that the business has adopted effective strategies to mitigate data-related risks. The last component of the framework is

governance which ensures that the strategies adopted by businesses to mitigate risks are utilized effectively and also adhere to the policies and regulations.

Various organization in the US have largely implemented the risk management framework to minimize the risks, which further helps in reducing the legal exposure and also aids in maximizing profitability. Not only this, but this framework when implemented within businesses also enhances being compliant with legal policies and regulations, improves data security and privacy protocols and much more. In addition, the framework also offers in-depth knowledge of what the organization needs in order to implement appropriate control and minimize risks when required.

The implementation of computing technology come with a lot of threats including issues of cybersecurity. Considering this as a major threat with the implementation of quantum computing technology within businesses, stakeholders emphasise on developing significant anticipations to help secure data privacy and security with businesses who have implemented these advanced digital tools (Jowarder and Jahan 2024). Enabling transformative advancements in different industries including smart healthcare, manufacturing, and virtual world. However, the shift towards transformation led to increased concerns related to trust, security, and risks that emerges with increased reliance of advanced technologies within these businesses. Thus, with the help of this framework, businesses with increased risks and threats can minimize these risks by ensuring regulatory compliance and acquiring expertise and knowledge of the technology in the specific field (Habbal et al., 2024).

The challenges of data governance in AI-enabled healthcare organisations. The study focused on understanding the complexities of balancing the technological advancements adopted by the healthcare organization with a focus on maintaining the privacy of patients. The study determined the increased need of strong risk management and data governance frameworks along with enhanced transparency, and public awareness that positively correlates with trust in data. Additionally, it also emphasizes on adopting flexible regulatory approach that helps navigate ethical and privacy concerns (Arigbabu et al., 2024). Risk management approach utilized by organisations during

uncertain conditions and circumstances result in enabling the organization to become more resilient and flexible. The impact of COVID-19 has left organisations with global turbulence that questioned the shift towards digital adoption. However, this implementation was not that easy and hence, organisations ensured to focus on their environmental, and socio-economic context. These further forced the organisations to consider the risk management approach in order to continue their business effectively while ensuring that the factors effectively address the sustainability issues. With a focus on operational, and risk management framework, the study emphasizes on analyzing the business operations and decision-making at different levels including its competitive scenario and systems ensuring on the security and privacy of data (Settembre-Blundo et al., 2021).

The adoption of digital technologies within businesses has driven the landscape of business, however, security and privacy of data concerns resulted in shaking the relationship between the customers and the businesses ultimately affecting the business profits. Thus, the increased need to prompt changes to regulate interventions for preventing consumers` data is highly required. This in turn helps in protecting the data and information provided by the consumers. Additionally, by incorporating the risk management framework, the organization can effectively create a foundation that help understand the implications of digital transformation in the protection of data (Quach et al., 2022).

The advancement of technology has increased the importance of communication and information in society. Everybody encounters data in some way, and throughout the years, access has expanded from one side of the world to the other. This has brought about fresh chances for everyone from one end of the planet to the other, but it has also brought about new difficulties.

Specifically, a global cybersecurity concern since data protection is typically a never-ending struggle. No matter where it is, data typically faces a variety of threats. This may expose a large portion of society, from individuals to international organisations.

Every nation in the globe should continually face the problem of data protection and work in coordination to collaborate with one another.

A decision that might bring nations together is to build a vast worldwide network that brings nations together. In order to figure out how to secure data, several sorts of concepts and techniques are put out in this manner. From one end of the globe to the other, certain regions have organisations that enforce stronger rules to protect data. For instance, Adopted by the European Parliament in 2016, the General Data Protection Regulation (GDPR) requires “companies to safeguard the personal data and privacy of EU residents for transactions that occur inside EU member states.”

Additionally, the GDPR governs the export of personal data outside of the EU. While the current emphasis is mainly on corporations, governments can directly develop a rule to give other countries with the opportunity to secure data nationally. Each nation has a separate set of techniques to secure data, which, in essence, makes building a big network feasible for everyone.

The rationale behind this is that, as previously said, it encourages nations to exchange their unique strategies for safeguarding data generated inside their borders. As a result, nations may gradually alter their data security practices to strengthen their defences. Additionally, it enables nations connected to the global network to learn more about other nations' data protection regulations. One such instance is Singapore, which "amended its personal Data Protection Act (PDPA)" to enable the nation to obtain the requisite data breach advices (Agrawal and Narain, 2019).

If rules similar to these are disseminated via a vast global network, it may inspire the creation of laws in other nations with different legal systems. Importantly, all nations collaborate to identify the best methods for data protection. Data is still being transferred daily from one side of the world to the other, and since this presents new opportunities and threats, it is crucial to keep this in mind. A crucial component of data protection is persuading nations to work together indefinitely, but global laws also need to be updated.

Not all nations are emphasising regulations to secure data better, despite the fact that more nations are becoming aware of cybersecurity and the ways, in which data should

be protected. It is necessary to implement rules safeguarding a variety of data in order for nations to collaborate more effectively. It will eventually reach a point when everyone on the planet will understand how important data protection is.

In general, 80 nations throughout the globe have laws in place to safeguard the privacy of data, and with government-crafted legislation, this number may rise. In the end, all data must be kept secure, but data also has to be shared globally to generate those opportunities. This considers new businesses to start, and it gives everyone the knowledge they need to go about their daily lives. Although data is shared, everyone in all nations should be considered as being safe since a wide variety of cybersecurity data should continuously be constant.

Many nations have enacted laws and regulations to protect security flaws and the use of PII (Personally Identifiable Information) by levying fines on businesses that disobey. The General Data Protection Regulations (GDPR) regulates the privacy of an individual's data both within and outside of a company. It puts obligations on businesses worldwide that target or collect data on EU people, despite the fact that it was created and implemented by the European Union (EU).

The Union of Europe created it and approved it. In her poll, more than 33% of the businesses lacked anti-spam and anti-infection protection, while others were virtually protected by simple measures such as server backup and reinforcement. The organisation's assets were not secured against a sophisticated digital assault since there was nothing in place to do so.

According to the evaluation, the participant's investments in IT security and cybersecurity are growing, and they are currently concentrating more on information security. Small and Medium-sized Businesses (SMBs) can benefit from GDPR by lowering the risk to their data security. He developed an online self-evaluation tool for small enterprises to ensure that they are adhering to GDPR regulations.

As we know the EU`s GDPR is an effective regulation framework that is used in organisations inside or outside the EU, it also offers SMEs with robust and tougher requirements that help process personal data and information without following any

adjustment protocols. With a focus on adapting the GDPR framework within SMEs, they can effectively comply with the regulations of GDPR. Additionally, the study offers a vast knowledge and understanding of the analysis and implementation design that help understand how organisations can work to achieve the compliance in order to protect and safeguard against cyberattacks, and data privacy and security (Brodin, 2019). By determining and reviewing the challenges of SMEs with the adoption of digital transformation, issues such as data privacy and cybersecurity occurred at large. Considering these issues as a major challenge, there is an increased need to focus on researching effective legal frameworks, and valid data encryption methods along with data acquisition policy and consequences that comes under the GDPR framework. This framework focused on differentiating ethical and legal challenges that deployed defensive data management strategies which ultimately relates to transparency and accountability within the internal business in order to deliver its customer with certainty and justice. Further, this helps isolate packet data to inform different levels of cybersecurity and data privacy issues (Wylde et al., 2022).

Cybersecurity is the most common issues that takes the form of data breaches due to the adoption of digital transformation within organisations. However, the organisations has largely adopted GDPR framework that robustly affects the issues of data breach within the organisations by complying with strict data protection rules. The Italian government derived the Italian National Framework for Cybersecurity and Data Protection from the NIST Cybersecurity Framework considering the significant aspects of data protection and cybersecurity (Angelini et al., 2020). Further, the utilisation of GDPR framework worked as an effective legislation that aided in reshaping the organisations based on data privacy and security concerns. This framework ensured to have a profound effect on the organisations` cybersecurity practices. In addition, the GDPR framework also introduced robust principles that were designed to safeguard customer`s rights and data privacy with a focus on considering transparency, accountability, and proactive measures that aids in preventing personal data. With this focus, effective strategies for addressing cybersecurity measures considering the role of

state and federal regulations can help design these strategies. This would further develop a deep understanding of the impact of GDPR framework on cybersecurity measures (Amoo et al., 2024).

GDPR framework is considered as one of the most stringent frameworks that are effective in the protection of data. This framework was passed by the EU with a focus on safeguarding the rights and freedom of all individuals, which ultimately focuses on the security and privacy of personal data and information offered by the individuals. The framework focuses largely on the cybersecurity aspects with main emphasis on state of art technology and encryption. The incorporation of the GDPR framework within organisations works as a primary method that aid in achieving compliance with the law while understanding the principles and tools for greater efficiency and cost-effective management of the information systems (Gobeo et al., 2022).

Following the Covid epidemic, a substantial knowledge gap on this topic was identified by the early literature analysis. SMBs in Middle Eastern countries such as Oman lack access to such a data protection framework.

2.2.2. Critical Analysis of Theories

According to the views of Silva (2015) the Technological Acceptance Model framework has been considered the best framework model to accept and utilize the technology effectively while determining the significant factors that are responsible for influencing individuals to make use of the technology. The TAM model by Davis emphasized on understanding the significant factors that result in affecting the performance of businesses based on their adoption of the novel digital technology. The model emphasized on explaining the integration of the technology by understanding the perceived usefulness that the business experience further resulting in enabling the business to perform better and become more productive as compared to its previous level of productivity. Not only this, but the use of this framework aids organisation in determining the external factors which involve the interface design, documentation, and training that result in affecting the perceptions of business owners regarding the shift towards digital transformation. In contrast to this, as investigated by Putri et al., (2023) the TAM framework is further used

to understand the effect on the security and privacy of data with an increased focus on the perceived usefulness of the organization based on the integration of the TAM framework that further leads to better and enhanced security of data and privacy of borrowers. Additionally, the framework also indicates a significant impact on the perceived usefulness of the digital adoption as it becomes quite use to use and also offers the organization with data security and privacy concerns. The sudden emergence that occurred during COVID-19 resulted in rapid shift towards technological innovations within organization affecting the daily lives of individuals as well as businesses. Thus, digital transformation became a savior for the businesses in the difficult times of the pandemic. The shift towards digital transformation has led to the integration of the TAM framework within organisations as it helps organization management to develop their understanding and enhance knowledge regarding the implementation and successful adoption of the digital technology. Based on the significant factors including awareness, knowledge, effective policies, social influence, demographics, compatibility, perceived risks, enjoyment, trust, and self-efficacy, the TAM framework works effectively.

Contrary to the above study, the findings of Alsyouf et al., (2023) emphasized on understanding the use of TAM framework that aids in managing personal health records of patients in the healthcare settings by ensuring that the data and information of the patients were not at the risk of threat. The study further determined that the management of personal health data of patients were influenced mainly by 3 important factors including the perceived usefulness, perceived ease of use, and security towards intention to use. All three factors of the TAM model aided in affecting the adoption of digital technology that determined negative usefulness and intention to use the digital technology within the organization. However, when utilizing this framework, the organization ensures to align the framework with the different business processes that promotes the ease of use of the technology. Further, the acceptance and intention to use the technology is mainly moderated the rules, guidelines, and policy of the organisation.

As the TAM framework focuses largely on the adoption of digital technologies making organisations and management develop their understanding about the technology,

there are several instances where organisations have to face issues and complexities that result in affecting them negatively. Thus, the NIST has developed the risk management framework which is developed with a focus on setting up policies for organization that aids in identifying the risks, eliminating and minimizing them. As opined by Jowarder and Jahan (2024), the risk management framework was developed to protect and prevent the US information system. In addition, the study also determined that the federal agencies have also adopted this framework that allows private organisation to adopt the technology as they have higher chances of posing risks and threats related to litigation issues, IT issues, and loss of capital. As the risks and threats are posed, the risk management framework is considered to be an effective framework which when integrated within organization can help reduce the risks.

Contrary to the above study, the study propounded by Arigbabu et al., (2024), focused on discussing the main components of risk management approach adopted by SMBs facing increased data risks or threats. It determined the key components involve the identification of risks, measurement and assessment of identified risks, risk mitigation, risk reporting and monitoring, and governance. All these components are considered important to eliminate the risks. For instance, many SMBs shifted towards digital transformation which in turn led to increased data security risks and cybersecurity risks, however, by utilizing this approach SMBs can easily determine the risks and implement appropriate measures by reporting, monitoring, and re-examining the identified risks to help the business take control of the security measures in minimizing the risks and adopting effective strategies that help eliminate risks related to data. At last, the businesses also ensures that whether the implemented strategies to mitigate these data-related risks complies with the government rules and regulations.

Despite so many frameworks and approaches cybersecurity is determined as one of the major global issue faced by organisations which is also considered as a never-ending struggle for them. This is so because the data faces significant threats that results in causing issues in data protection and work by coordinating and collaborating with the adoption of significant data protection frameworks. One such framework is the EU`s

GDPR framework which offers SMBs with the right to prevent and safeguard the personal data and information of the customers based on their transactions. As opined by Brodin (2019) SMBs require robust data requirement to adjust the data and information by complying with the adjustment protocols. The GDPR framework when integrated within organisations offers a great understanding of achieving compliance with the framework to safeguard data against cyberattacks, and data security.

Contrary to the above study, the findings of Wylde et al., (2022) emphasized on identifying the challenges faced by SMBs because of digital technology which requires an increased need of legal frameworks and data encryption methods. The GDPR framework involves the data encryption and acquisition policies which are effective in addressing the legal and ethical issues related to data while deploying effective data management strategies. While the study propounded by Angelini et al., (2020) focused on explaining that the GDPR framework not only addresses encryption issues and digital problems but also stand against cyberattacks and issues. It involves a robust GDPR framework to address the issues of data breach by adhering to the data protection rules and policies while complying with the set rules and regulations.

In contrast, according to the findings of Amoo et al., (2024) the GDPR framework work as an effective legislation that reshapes the organization by determining the issues related to data privacy and security. Significant principles were developed under the framework to protect data and customer`s rights ensuring that the SMBs comply to the framework focusing on accountability, transparency, and proactive measures.

2.3. Main Research Variables

2.3.1. Impact of digital transformation on the organization’s data related problems in small and medium sized business

2.3.1.1. Introduction to digital transformation

Nowadays, the digital technology serving as a pillar for every business and this has grown with the advent of high speed of internet and with the introduction mobile phones along with other digital devices such as computer, laptops, etc (Vermesan and Friess., 2022). Thus the initial wave of digital transformation was marked by the adoption

of basic computing systems, that are specifically email communication and through various websites.

Digital transformation which refers to the process where businesses of every sizes adopts digital technology into their operations (Ulas, 2019). This also allows business in reducing costs, increasing efficiency and streamlining business operations in this rapidly evolving business landscape. Overtime this technology has become a significant part of every business due to its efficiency and thus has revolutionized the way the businesses use to perform earlier. In addition to this advent of high-speed internet has increased the usability of mobile phones, and this has influenced majority of the businesses to revolutionize their business operations. With the digital transformation companies get empowered to quickly respond to any sort of change in market demands and hence allowing them to adjust their strategies in no time (Garzoni *et al*., 2020). Thus, allowing them to attract large pool of customers towards them with their pivot strategies. And this influenced business to embrace such digital technologies in order to reach global audience.

Such digital technologies involve cloud computing, artificial intelligence, big data analytics and the Internet of Things (IOT). All these digital technologies empower business to enhances their functionality, improve efficiency and thus further allows creating new value proposition in the competitive business landscape (Chander *et al*. 2022). Each of these technologies provides unique services companies and thus facilitate them in different operations. Specifically, cloud computing technology enables businesses to access scalable and cost-effective IT solutions and thus allows businesses for reducing reliance on physical infrastructure. AI-powered technologies and big data analytics empowers business to with predictive insights and automation capabilities. And lastly IoT devices allow businesses to track inventory, monitor equipment performance, and optimize logistics.

The evolution of digital transformation brings more businesses to implement emerging technologies for competitive gain. The vital aspect of business transformation

relies on blockchain technology because it delivers enhanced transparency alongside heightened safety measures and efficient operational performance. Blockchain technology delivers maximum benefits to managing supply chains and financial operations and safeguards data by providing impenetrable records that prevent corruption and fraud according to Nakamoto (2008). Blockchain adoption by Omani SMBs allows decentralized data management through decentralized solutions which lessens their dependency on traditional centralized systems while reducing cybersecurity threats.

Businesses today require exceptional attention to cybersecurity alongside data privacy because they continuously accumulate large quantities of customer information. Businesses sustain mounting pressure to establish deeply protective data security protocols because consumers and regulators intensify their concerns about data breaches and compliance requirements (Von Solms and Van Niekerk, 2013). The Personal Data Protection Law (PDPL) in Oman requires businesses to establish data governance policy compliance while securing customer information and strengthening their cybersecurity frameworks. Organizations must deploy strong encryption protocols along with robust access control systems to stop illegitimate access to sensitive information because cloud services have become increasingly important. The digital evolution substantially changes both the corporate leadership environment and team operational methods. Moving toward digital operations demands that employees build new technical abilities while adjusting their skills in dynamic business settings. Today's workforce needs digital skills and continuous training as basic requirements to succeed in modern technological office environments (The Fourth Industrial Revolution, 2017). Modern businesses support digital training initiatives that create continuous learning conditions to close the difference between traditional work methods and contemporary technological standards. Rapid technological adoption faces significant obstacles for SMBs operating in Oman mostly because of their limited financial capabilities.

Industrial Revolution 4.0 uses robotic process automation and automation technologies to minimize human errors and optimize productivity levels (Aguirre and

Rodriguez, 2017). The automation technology RPA helps companies from multiple sectors enhance operational efficiency by managing functions including invoicing customer support and supply chain administration. Through automation technology businesses enhance operational productivity and free their workers to pursue tasks that demand critical thinking alongside innovation. Omani small and medium businesses should embrace automation to provide better services at reduced operational expenses.

2.3.1.2. Small-Medium Sized Businesses and the Adoption of Digital Transformation

Small-Medium Sized Businesses refers to the business sectors that are smaller in size and they earn lowered revenues due to limited infrastructure and financial constraints as compared to large scale business (Bisht and Singh, 2020). Although these are small business but they plays a crucial role in economic growth, innovation and job creation. In Oman, SMBs are a vital part of the economy and are known to operate in various sectors which includes, retail, manufacturing, tourism, healthcare, and technology. These SMBs are known to make a large contribution to the GDP and also in increasing employability of the country. It has been found that SMBs in Oman make a 33% of contribution to GDP and 45% contribution to employment (Khalifa, *et al.,* 2022).

SMBs have been significantly influenced to adopt digital transformation due to the challenges posed by the COVID-19 pandemic (Muthuraman, *et al*., 2021). As the outbreak of the COVID-19 had forced many businesses to shut their business down due to lockdown and restriction in movement the businesses were left with no option rather than shifting to e-commerce, online payment system and cloud based platform in order to sustain their business in that crisis. Operating and continuing business in traditional business model was not possible at that time. On the other hand, the easy accessibility of the system and increased demand of the customers for digital existing business or e-commerce business has forced every business to adopt digital transformation and thus SMBs are not an exception to adopt this digital technology. Also the rise of customer demand for digital services has further influenced SMBs to innovate and embrace this

new emerging technological advancement and thus has also contributed increasing employment (Busaidi et al., 2022). With an increasing number of customers preferring online transactions, mobile applications, and digital customer engagement, SMBs had to integrate new technologies to remain competitive. Thus, from the COVID-19 period businesses moved more towards digital transformation and even in 2025, companies are relying on digital technologies allowing businesses to access data remotely, facilitating seamless communication and collaboration among employees.

In addition to this the various government polices has also influenced digital transformation in Oman such as Oman Vision 2040, which emphasizes the adoption of technology and innovation to drive economic diversification. Government initiatives such as Invest Easy, the National Program for Digital Transformation, and support from institutions like the Oman Chamber of Commerce and Industry (OCCI) have encouraged SMBs to embrace digital tools (Al Balushi, 2019). In addition to this the financial incentives, regulatory support, and digital training programs have also played a key role in accelerating this transition. Apart from this the intense competition from the large size businesses further influences them to adopt digital transformation. Thus, this can be said that the transformation has proven to be a crucial step to sustain sustainability and growth for the SMBs in Oman.

The increase in the availability of digital structures is the primary reason that contributes to the current advancement of digital transformation in Omani SMBs. Oman's government has especially embarked on the Vision 2040 strategy where it has invested in high-speed internet, cloud, and Fintech (Al-Sartawi, 2021). These provide the SMBs with the groundwork for integrating digital solutions in their operations, like e-commerce, and CRMs, digital payment services. Also, the emergence of COVID-19 forced consumers to order their products online hence promoting other businesses and organizations to adopt the online platform to compete with the modern market (Al Badi et al., 2022). The other key factor is the continued expansion of financial technology sometimes called mobile banking. Increased adoption of mobile wallets and blockchain-facilitated transactions as

forms of payment solutions are modernizing the operations of SMBs (Mohamed, Bakar, 2023). In terms of innovation, the use of fintech solutions in Omani SMBs is aimed at efficient management of cash flows, funding opportunities, and transparency. Other developments in the technologies that include cloud accounting software as well as the use of Artificial intelligence in performing financial analysis are also helping SMBs make better decisions based on data (Al-Muharrami, 2022).

However, the reality is that some challenges prevail in digital transformation among Omani SMBs. There is, however, an important problem of relatively weak financial resources and investment activities among numerous small businesses. While other big organizations can have large capital outlay for physical structures or invest a large amount of money on advanced technologies such as IT or cybersecurity automation and cloud computing services, the constrained financial resources of SMBs often restrict them from affording such technological requirements (Al-Farsi and Al-Kiyumi, 2022). This impacts the acquisition of financial resources by businesses hence slowing down the uptake of digital technologies, thereby, making them use ineffective technologies that slow down their operations. One more issue is the lack of digital competencies of the employees and owners of private enterprises. According to the literature, it was found that a high percentage of Omani SMBs were not capable of deploying and managing digital technologies proficiently (Khan et al., 2021). Concerning the identified threats, the lack of digital skills results in the use of consultants and, therefore, high levels of operational costs. However, there is one more important factor that hinders a fast transition to digital, and it is the employees' resistance to change. This is most apparent in family businesses where hierarchy tends to hinder the adoption of change (Al-Gharibi and Al-Wahaibi, 2023). There is no doubt that many other factors have also continued to pose a great threat to information technology; cybersecurity is among the most critical, which slows down IT adoption. SMBs (Small and Medium Businesses) do not fully adopt digital solutions for several reasons such as data breaches, cyber-attacks, and compliance concerns (Sultan and Al-Salmi, 2022). Implementation of Oman's Personal Data

Protection Law (PDPL) to meet more stringent legal compliances becomes an additional compliance challenge to the organizational endeavor toward digital transformation.

To address these issues, several initiatives can be adopted to enhance the process of digital transformation in SMBs operating in Oman. It is seen that the role of government here with their initiatives and with their support from the financial front are important in trying to overcome the digital divide. Officially, the Omani government has enacted several funding strategies, training interventions, and tax credits that SMBs can leverage to enable them to integrate digital tools (Al-Sartawi, 2021). There are opportunities for further development of such activities and an increase in funding availability for early childhood education to support the process of digitalization throughout the sector more extensively. Another primary source of intervention is skill development in the area of computer literacy. It is also stated that offering training workshops along with certification programs, as well as digital education courses can contribute to the construction of an internal capacity for SMBs in the management of digital tools (Khan et al., 2021). In recent years there have been specific actions that link representatives of industries, universities, and other related local and global institutions to share knowledge on how to develop SMBs' digital capabilities. Moreover, cloud and easily scalable digital solutions can be useful in helping SMBs integrate their operations digitally step-by-step. SaaS and cloud computing combined with automated intelligent services facilitate the incorporation of digital processes in organizations in the most efficient and economical ways (Al-Muharrami, 2022). Well, the above-listed technologies offer manageable solutions in the market that can be accommodated by most of today’s SMBs and do not demand large amounts of capital to acquire.

The digital transformation of SMBs in Oman is gradually progressing due to enhanced digital connectivity, fintech advancements, and a shift in customer behavior. However, some factors like limited resources and funds, inadequate skills in the use of Information Technology, and threats such as hacking have remained as factors hindering this evolution. To achieve a sustained level of digital integration, governments need to

advocate for the sector, individuals need to enhance their knowledge, and affordable technologies should be availed. In this way, it is crucial for Omani SMBs to adopt such strategies for success and to improve their presence and relevance in the digital economy.

2.3.1.3. Scope of Digital Transformation

Such advancement in these digital technologies acts as a critical factor for enabling growth and competitiveness for the business. In this competitive business landscape the digital transformation for SMBs is not only a move towards technological advancement but it acts as a strategic movement that empowers them redefine customer experience, internal operations and their overall business models (Oladimeji., andOwoade., 2024). As SMB refers to small-medium sized business it is known that they have limited infrastructure and resources which restricts them in gaining significant completive advantage with the large size businesses by implementing digital solutions that streamline operations and enhance scalability. With the adoption of digital transformation it has opened up many opportunities for the businesses in several dimensions such as it has facilitated in offering best customer experience, business model innovation, data driven decision making scope and also this allows them to increase their productivity.

In this competitive business world, customers are the backbone of the companies which allows them to earn significant revenues through best customer experience. As customers has handful of businesses providing the best customer experiences has become priority of every sizes irrespective of their sizes and thus SMBs are not an exception to adopt these emerging digital technologies. SMBs that leverage digital transformation through digital marketing, social media, and AI-driven analytics enhance customer engagement and satisfaction (Deep and Zanke., 2024. Also, this allows them to create their presence in the virtual world of business thus allowing SMBs to reach broader audience segment. Thus, this allows them in transitioning traditional business model to hybrid business models. In addition to this, with the advent of artificial intelligence, this derives insights from the real-world scenarios and thus this allows recommending

product that are in high demand in the market. Furthermore, with the adoption of digital transformation, this allows for automating the tasks and this allows for reducing operational costs or the SMBs.

Although with the path of digital transformation offers multifaceted benefits to the SMBs but as every digital technology has their two sides one is the positive and the other is the negative side. Businesses that adopt digital transformation are exposed to various data security challenges. Thus, this can be said that the digital transformation presents opportunities as well as threats for the SMBs. The adoption of digital transformation forces SMBs are exposed to cyber security threats, data breaches, and compliance with evolving regulations, which can be overwhelming due to limited financial and technical resources (Papathanasiou *et al.,* 2024). Even if the system has become a necessity for the small and medium-sized businesses (SMBs) in Oman but embracing allows them face challenges related to the digital vulnerabilities.

Digitization is not limited to just optimizing processes and underlines the transformation of small and medium size enterprises (SMBs) in Oman in terms of capabilities and strategies for competition and growth in the digitalized environment. However, one of the key aspects of this transformation is that it has hit the button for SMBs to use digital platforms for market growth. Due to advances in the application of e-commerce solutions the effects of cloud-based ERP systems and several payment gateways, firms can enter the global market without a physical location (Al-Karousi et al., 2023). This aspect means that while expanding their business online, SMBs can reach a broader audience of customers, and expand their range of services without substantial investments, which would have been necessary if the companies were made to open physical stores for their businesses. In addition, agility and resilience are other elements within SMBs where digital transformation has a significant influence. Cloud computing for instance enhances distant working which allows organisations to operate effectively even if there are external challenges such as economic fluctuations or other specific disturbances (Sharma and Jain, 2023). This increases flexibility and speeds up the

operations of SMBs whenever there is a change in market, customers, and competitors to enable sustainment in the ever-evolving digital environment. Other areas that may warrant automation include replenishment of stored products, customer response through the handling of queries through the use of bots, and invoicing all of which cut out on human error, and increase, precision and effectiveness.

Another kind of influential factor, that is regarded as a part of digital transformation, is big data analytics. Thus, by obtaining effective utilization of data analytics, SMBs can proceed with an effective decision concerning customer choice, supply logistics, and demand. Self-service technologies assist consumers in finding related products, assist in the timely determination of the appropriate pricing of products for maximum profitability, and can help businesses improve their products to achieve greater satisfaction among their consumers (Jain et al., 2024). This impactful data gives the SMBs ways to work smart and efficiently, thus, counteract the large companies. At the same time, it is critical to note that digital transformation brings about its own set of challenges related to digital literacy along with the challenge of upskilling the SMB workforce. Small businesses struggle to follow new technologies because they do not access quality employees or have sufficient knowledge about implementing new technologies (Abu Zayyad and Al-Khouri, 2023). This study pointed out that by training staff and implementing financial support the possibility of successful application of digital training within SMBs can be enhanced while minimizing the reasons for digital resistance.

2.3.1.4. Digital Vulnerabilities

Small and Medium-Sized Businesses (SMBs) in Oman face several digital vulnerabilities that seriously jeopardise their operational integrity and data security as they quicken their digital transformation in reaction to the COVID-19 epidemic. And this further has a significant negative impact on the stability and prosperity of these companies. One of the biggest risk of the digital transformation that majority of the business in all across the world is facing is the cyber threats (Tekic and Koroteev, 2019).

Business on moving towards digital platforms, this mandates them to store sensitive data related to the customers and business, making them attractive targets for cybercriminals. Phishing attacks, ransom ware, malware, and hacking attempts have become significant threats to business globally. But the SMBs are considered to be the most sufferers due to their weaker financial condition and limited infrastructure. And majority of the SMBs in the Oman are facing such challenges due to their inability to implement robust security protocols which can empower them to avoid such malware activities (Tekic and Koroteev, 2019).

Apart from this one of most significant digital vulnerabilities that the SMBs are facing in this evolving digital landscape is due to the adoption of inadequate cyber security measures. Implementing robust cyber security protocols as demands for a healthy financial condition but as SMBs are restricted with financial constraints this does not allow them to implement robust cyber security protocols, and they are forced to expose to such malware activities. And this further leads to cost them high charges. Avoiding such protocols when leads to ransom ware, malware and phishing scams, through hacked websites which leads to data theft or data damage. Thus, although the adoption of digital transformation has empowered the SMBs in multifaceted ways, but the negative effect of this digital transformation is a big threat for the SMBs in Oman. Ransomware, often leads to data encryption and may lead to data lock and to some extent this may also demand for a fee to unlock it. On the other hand, phishing attacks often demands for human involvement, a study by Perwej et al. (2021), has defined that the that cybercriminals exploit human errors through deceptive emails and malicious links, leading to financial and data losses. And thus, this shows a pressing need for providing training to the employees to mitigate such risks. In addition to this addressing such threats require for a strategic approach with a comprehensive technological solutions and employee's awareness the SMBs in Oman can significantly fight against such digital vulnerabilities. At the phase where SMBs in Oman plays a significant role in generating employability, reducing poverty, labor absorption and contributing significant to the GDP

of the country, facing such digital threats is a challenging situation for them which may also hinder their growth.

Apart from this as in post pandemic situation, majority of the customers are giving priority online platforms or e-commerce business models, and in order to attract such customers towards the brand SMBs in Oman has also taken their baby steps towards this digital transformation, but due to this they are facing devastating consequences. Due to financial constraints, they face the challenge of data backup and recovery plans. As the cyber-attacks firstly had an impact on data inadequate backup system may lead them to face consequences of data loses Kumar (2023). And thus, there shows a need for implementing robust data backup systems this will ensure all the important data have backup and are stored in password protected device and can be recovered or restored in uncertain situations

Further SMBs in Oman face significant challenges due to network security vulnerabilities, primarily stemming from weak firewalls, unauthorized systems, and unsecured Wi-Fi networks (Corbett-Wilkins, *et al.,* 2023). Continuing organizational operations with such common networks are harmful for the SMBs and thus they are susceptible to unauthorized access and attacks. And with such flaws in the system the hackers take advantages and enters internal networks and hacks all confidential data of the companies. Again, with limited budgets and limited experts the SMBs are exposed to data breaches, financial losses, and reputational damage. In addition to this, SMBs are also in the risk to flaws in access control, as the access is allowed to authorize people. And on the other hand, if access remains with the employees, then the excessive access also led to unintentional data leaks. But in order to mitigate this risk or to reduce this risk, the SMBs has the option to implement Role Based Access Control (RBAC) and also to take more preventive measures one can also adopt multi-factor authentication (MFA) offers an additional layer of protection. Another significant vulnerability that the companies had to face is the vulnerability to unpatched software and outdated system which also give license to the hackers to exploit company's security and confidential data (Ngonga, *et al.,* 2019).

Furthermore, compliance with data protection regulations, presents an additional challenge. As SMBs are not allowed to follow all the laws and rules, including norms like the General Data privacy Regulation (GDPR) and local legislation in Oman. And this may lead the company to face reputation loss. Overtime, all the cyber-attacks have become an alarming phenomenon and thus making this more challenging for the SMBs to operate their functions smoothly and without having the risk to data vulnerabilities. Moreover, third party vulnerabilities also pose risks as majority of the business had to rely on vendors and partners due to their limited financial budgets thus increasing a chance of weak security which can lead to supply chain attacks (Ilori et al., 2024). Thus, due to these impacts, SMBs had to face financial losses, reputational damage, loss of customer trust, and potential regulatory penalties. Without proper cyber security strategies, SMBs in Oman remain at high risk of cyber-attacks that can disrupt business growth negatively and to some extent may also force them with no option other than taking drastic step to take a leave from the market.

2.3.1.5. Attackers' steps to digital vulnerabilities

The adoption of digital transformation plays a role of organizational development strategy for the SMBs, where this allows them to believe that this will give them a high return, but something is happening in totally an opposite way. Although the digital transformation is not a new agenda it has been in trend since several years, but the significant or rapid transformations has taken in action since from the arrival of corona virus and lockdowns. Where the SMBs has chosen this path to grow their business to a higher level and attract a large pool of customers with their digital presence, whereas hacker took this as an opportunity to hack all confidential data.

Attackers, however, typically start with crude and outdated techniques of assault before becoming more sophisticated when the effort is worthwhile. Lack of basic protection and digital “hygiene” makes many firms, particularly the smaller ones, vulnerable to simple assaults. Targeting companies that have already attained this baseline

level tends to be the focus of more advanced strategies. Attacks involving phishing, denial of service, and ransomware are still common in the digital world.

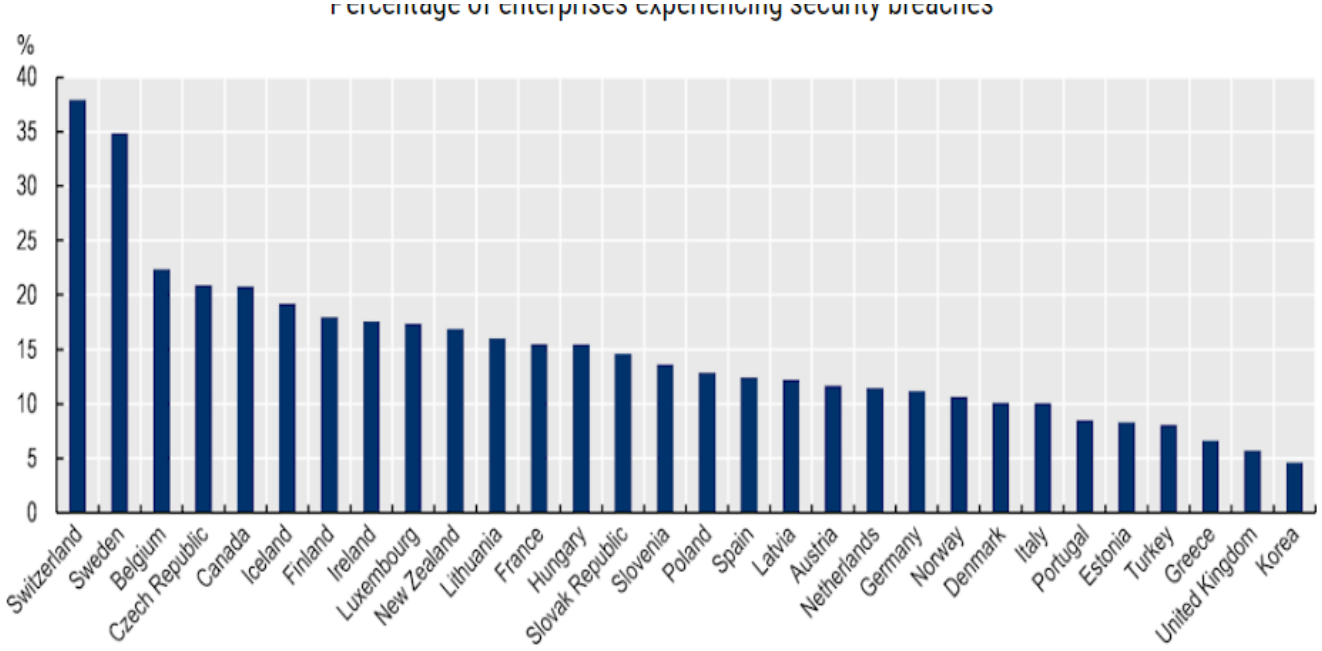


Figure 2.1: Percentage of enterprises experiencing security breaches

(Source: OECD, 2020)

Data is more prevalent than ever, and its digitalisation has turned it into a strategic asset. An increasing amount of data is generated throughout business activities, such as the production and distribution of items (process data), and is gathered at different stages of business interactions (user, consumer, and supplier data). Process data may enhance inventory control, maintenance and operations, and corporate responsiveness to last-minute demand development.

Additionally, they broaden the range of efficiency gains in terms of resource and energy utilisation. Data from users, consumers, and suppliers is crucial for understanding the market, further enhancing customisation, and embellishing new products and business models. The quantity of data generated worldwide is expected to expand at a compound annual growth rate of 61 percent, from 33 zettabytes in 2018 to 175 zettabytes in 2025 (Habibzadeh et al. 2019).

How SMEs safeguard their data is becoming increasingly important in this situation. Trade secrecy is frequently prioritised as the primary method of data security by SMEs. Trade secrecy is the term used to describe proprietary business information, such as enhanced recipes, new manufacturing processes, firm strategy, or commercial knowledge about who to sell to and who to buy from (e.g. client list). Trade secrets, as opposed to patents, are protected by laws governing the secrecy of information, such as confidentiality agreements, non-disclosure clauses, and covenants not to compete. Because trade secrets are so common and there are no official registration requirements, they remain relatively usable, reduced organisation expenses, and lack of a set period of protection. The safeguarding of trade secrets has become more challenging as an outcome of digitalisation. The revolution in data codification, storage, and interchange (cloud computing, emails, USB drives, etc.) is primarily responsible for the rise in trade secret violations.

Increased value placed on intellectual property (and consequently, its unauthorised use), staff flexibility, shifting work environments and working arrangements The fragmentation of global value chains (with more foreign parties participating in various legal systems and uneven enforcement circumstances), as well as short-term contracts, outplacement, and teleworking, all enhance the danger of disclosure.

One of the several vulnerabilities that SMBs must deal with is Windows kernel security issues. It is one of the major security issues. Attackers alter certain data files in the Windows kernel to prevent the detection of malware drivers and to increase their level of system access. Information about a loaded driver is kept in a number of system records, which are composed of allocated components connected by linked records. The malware driver's structure can be removed by attackers from these categories to render it inconspicuous.

There is another opportunity for user data problems. Almost all SMBs kept the data on digital devices, often, hard drives, after the coronavirus epidemic. Malware, for instance, has the ability to steal or destroy encryption data, which is utilised in cryptography modules and may be used to decrypt user data. Malware can also jeopardise a user's privacy by collecting Windows investigation and other data obtained by the

Windows operating system (GDPR, 2020). The security system should be able to prevent unauthorised access to Pound data that is temporarily allocated by outside drivers.

Last, malware that targets industrial control software has the potential to do serious harm. A well-known instance of kernel-mode malware called Stuxnet was in charge of wiping out 1000 centrifuges at Iran's nuclear plants. Its driver was specifically designed to work with Windows-based Industrial Control Systems (ICS), which are frequently paired with Siemens PLCs.

A related attack vector for cyber-attacks is software for computer numerical control (CNC) machines, which use computers to drive various industrial devices including lathes, grinders, and piercing machines. CNC machines are frequently used in high-end production; for instance, NASA, Boeing, and SpaceX all use them.

2.3.1.6. Threats to Data Protection

The outbreak of the COVID-19 in the late 2019 has profound impact on the business world, its negative impact on the physical health and life-threatening symptoms has made possible to all those activities which once thought to be impossible. Thus, to maintain contactless operations businesses were left with no other than moving towards online virtual presence (Stalmachova et al., 2021). But the shift in the business model opened new threats and challenges rather than the opportunities. And SMBs faced more challenges as compared to the larger companies because the small size business is not much familiar with the digital technologies, and they have limited hands on experience with digital technology. In addition to this organizational readiness to adopt digital transformation was seen as significance challenge and this had allowed making the company data as a crucial data (Omrani et al., 2023). Thus, a situation where companies are operating their functions remotely and where employees share their personal data with the company securing such confidential data becomes a priority for the companies irrespective of their sizes. But at the same time securing those data becomes more complicated and costly for the SMBs. But with time as the presence of remote work got an importance the business world got chance to get introduce with different technologies with

which the company can store all the confidential data with security. Such technologies involve virtual servers, cloud environments, and on-premises data centers. This shift has introduced new challenges in data management and security, highlighting the need for robust strategies to protect sensitive information in an evolving digital era.There have never been stricter performances SLA1s or harder legislative commitments. IT teams are expected to save costs and "do more with less" as the difficulties associated with SMB data security grow more difficult to manage. Data leakage in the Middle East tripled during the crucial months of the outbreak. The most impacted sectors were coordinated factors, healthcare, energy and utilities, aviation, government, and retail.

Sources	Trends
Canadian Federation of Independent Business (4 May 2020)	Of the 26% of business owners who had online operations prior to the COVID-19 crisis, 30% have seen an increase in sales.
US Chamber of Commerce (5 May 2020)	Over April-May 2020, the share of small businesses transitioning some or all of their employees to teleworking increased from 12% to 20%, and the share of small businesses that had begun moving the retail aspect of their business online increased from 10% to 17%.
Pew Research Center survey (late March 2020)	40% of adults aged 18 to 64 in the United States reported they had worked from home as a result of the COVID-19 outbreak, as compared to estimates of 7% of private-industry workers and 4% of state and local workers who had the option to telework prior to the pandemic.
McKinsey (Germany)	Whereas at the outset of the crisis, 88% of German SMEs operated with mandatory in-person work, 81% expect that the pandemic will make their companies more flexible and one-third of SMEs esteems digitalisation has grown in importance due to the pandemic.
IBM/Ponemon (August 2020)	76% of survey respondents said remote work would increase the time to identify and contain a data breach. 70% of respondents said remote work would increase the cost of a data breach.

Figure 2.2: Early evidence of the impact of the COVID-19 on business digital adoption and risk

(Source: OECD, 2020)

2.3.1.7. Challenges for SMBs

Cybersecurity dangers may affect small organisations just as much as they do bigger ones. Small businesses sometimes believe they are too unimportant to be the focus of hackers, but this is untrue. Automated assaults may really target many small businesses at the same time. These companies frequently lack the means to invest in cybersecurity, have less knowledge of possible threats, and have poorer technology

defences. As a result, they are often easier targets for hackers compared to larger organizations, despite being equally attractive due to their financial assets and valuable customer data that must be protected under regulations like the GDPR.

Furthermore, small businesses often serve as intermediaries for larger companies, making them potential stepping stones for cyber-attacks aimed at bigger firms. Consequently, small businesses frequently bear the brunt of damaging cyber incidents. Research indicates that companies with fewer than 500 employees experience average losses of $2.5 million per cyber-attack (Doyle et al. 2020). Beyond the financial impact, the reputational damage from such breaches can be severe. The challenge of adapting to a digital business model can be compounded by differing executive perspectives on environmental changes, making it difficult for management to develop a unified approach to these challenges.

2.3.1.8. Recent attacks on SMEs

Start-ups and SMEs are increasingly susceptible to cyber-attacks due to their inadequate security measures, which can be exploited even through routine communications (Fahmi et al. 2020). A recent report by the Cyber Peace Foundation, the world's first non-profit organization focused on mitigating cyber threats, reveals that 43% of cyber-attacks target small businesses and start-ups. This highlights the urgent need for these businesses to develop robust cybersecurity frameworks.

Start-ups and small businesses often operate on a limited scale with constrained resources. Consequently, enhancing cybersecurity is frequently deprioritized compared to business expansion. According to the report, about 46% of SMEs lack a clear strategy for managing cyber threats. Moreover, nearly 60% of small businesses that fall victim to cybercrime fail within six months. SMEs and start-ups are notably more vulnerable to cyber-attacks than large corporations due to their limited resources for implementing top-tier security measures. Cybercriminals are attracted to the lack of sophisticated security

guards, monitoring systems, and advanced access controls in these smaller enterprises, making them easier targets.

Cybercriminals might shy away from breaching the heavily fortified networks of large corporations due to the extensive security measures in place. Consequently, SMEs and start-ups often become the preferred targets. Additionally, small businesses may underestimate the value of their data, assuming that cybercriminals will focus on larger targets or consider their data insignificant.

The COVID-19 pandemic has underscored the profound changes in the business environment. Over half of the businesses recognize the need to act swiftly to mitigate the long-term impacts of the pandemic. Adapting to a digital business model has been one of the most challenging tasks during this period. Thus, this has necessitated the need for a strong short term and long-term strategies to navigate the consequences the crisis situation. As digital security incidents my offer a serious repercussion for the companies, governments and individuals, affecting the accuracy, accessibility and privacy of data. Some of the common attacks that majority of the business had to face the consequences of is involves:

Phishing Attacks

Phishing attacks have become one of the most prevalent cyber security threats in the digital age, particularly affecting small and medium-sized businesses (SMBs). Phishing attack involves cybercriminal who use to hack company's confidential data and leaks sensitive information, such as login credentials, financial details, or personal data, by impersonating legitimate entities through fraudulent emails, websites, or messages (Sonowal, 2021). Although Phishing is not an new phenomenon the landscape of business is familiar with such malware activities but the post-pandemic era has witnessed a surge in such attacks, significantly impacting SMBs that often lack the robust security infrastructure of larger enterprises.

It has witnessed that the phishing has witnessed an increase of 65% in the last 12 months, which has lead to a loss of over $12 billion. This huge figure highlight that he phishing have evolved as a complex thing in the recent years and attackers. In addition to this Business Email Compromise (BEC) has also increased, wherein cybercriminal target high-level executives with phishing schemes to obtain their passwords, and further with the help of these credentials they do fraudulent activities with the employees. Also the figure has increased to such numbers because even in the post pandemic situation companies have not switched to complete physical offices and there are many offices which continue with hybrid work mode and permanent work from home mode. This has resulted in an increase in cyber threats as employees working from home often accessed corporate systems through personal devices or unsecured networks. And the cyber criminals have taken the advantage of it and have exploited the situation by targeting the SMBs particularly. In addition to this, the rise of social engineering tactics, business email compromise (BEC) attacks, and ransomware delivery through phishing emails has intensified the risks for SMBs. One of primary reasons behind increasing this phishing attack is the increased rely on email communication in such working mode where employees had to communicate and collaborate through mail (Al-Qahtani and Cresci, 2022). And as SMBs are not equipped with expertise IT security team they fail to detect phishing attempts and cyber criminals find this easier to target the SMBs.

Phishing attacks have significant consequences for SMBs which may initially lead to financial losses. As SMBs often operate with limited financial resources, this makes them vulnerable to cyber fraud. And to some extent this may also pose the challenge of monetary theft through fraudulent transactions. Further data breaches are another significant challenge of which results from unauthorized access to sensitive customer and employee data and also such breaches can lead to compliance violations Neto et al. (2021). Also inadequate data security system also significantly leads to losing customer trust and thus affects an SMB’s reputation. Thus unlike large enterprises SMBs find it challenging for to recover from the reputational fallout, impacting customer retention and business growth.

Malware Attacks

Malware is another significant risk to small business where the cyber criminals create harmful code to steal information by entering through different networks (Goni., 2022). The hackers commonly attack the companies via spam emails, malicious website downloads, and connections to other compromised computers or devices. Thus, these attacks are especially harmful for the small sized business due to their inadequate and robust systems and also cost them a high charge to get out of its effects. Furthermore, the attackers to some extent also bring challenges for the companies by pushing their clients and employees at a high risk.

However, personal devices are more likely to be vulnerable to malware attacks since they are more likely to be the target of fraudulent downloads. Businesses may stop malware attacks by implementing security measures and concentrating on these areas. In addition to shielding computers from virus downloads, endpoint protection solutions give the chairman a single control panel to manage devices and ensure that everyone's security is up to date. Web security is important because it shields users from accessing rogue websites and installing rogue malware.

Ransomware

Ransomware is one of the most well-known cyberattacks, impacts a significant number of companies. These attacks have recently increased in frequency because they are among the most profitable types of attacks. Ransomware encrypts corporate data, making it unusable or unreachable, and then demands money from the organisation to unlock the data. As a result, businesses must decide whether to pay the ransom and risk losing large quantities of money or to risk losing data and endangering their services.

Small businesses are especially susceptible to attacks of this nature. Ransomware assaults, which demand an average payment of $116,000 per victim, are reported to target 71% of small businesses. Attackers know that smaller businesses are far more likely to pay a ransom since they often don't have backup data and must evacuate immediately. The healthcare sector is especially vulnerable to this type of assault since it may force a

company to make the decision to close or not until a payout has been received by locking patient medical records and appointment schedules.

To prevent these attacks, companies must concentrate on strengthening their areas of strength and implement security measures across all company equipment. These will help reduce the likelihood that ransomware attacks would successfully encrypt data. An endpoint security product called Sentinel One even has a “ransomware rewind” feature that helps companies spot and stop ransomware attacks right away. Companies have to consider implementing a dependable cloud backup system as well.

These technologies lower the risk of data loss by securely backing up enterprise data to the cloud. There are many different data backup methods available to organisations, so it’s critical to choose the one that will be most effective for your business. IT teams may quickly restore their data in the event of a ransomware attack without incurring any expenses or losing productivity by implementing data backup and recovery. This is a significant breakthrough in cyber-resilience.

Thus, although the digital transformation has empowered the businesses for continuing their operations digitally, but it has offered multifaceted challenges relate to data breaches, financial loss, reputational loss etc, for the SMBs in the Oman in the post COVID-19 scenario.

2.3.2. Data-related issues faced by Organization management leading to inadequate security and technical progress

2.3.2.1. The concept and significance of Data protection for Organizations

Data protection has become a significant part of every organization irrespective of their size at the emerging phase of digital transformation. Thus, this refers to the process wherein the companies take up the responsibility to keep all the confidential data of their employees and customers securely, so that it doesn’t get revealed or leaked outside the companies. Also, as different companies have unique strategies and goals, the companies also keep their confidential data secure and safe so that nobody other than them knows about their aims and goals. And in the post COVID-19 period, as the majority of the

business has adopted this new trend of digital transformation in order to compete in this business landscape, thus data protection has become a significant part of the companies.

A novel aspect of data protection theory involves making sure that data can be quickly restored after any degradation or weight (Habibzadeh et al. 2019). Other crucial components of data protection include ensuring data security, protecting data from put out some reasonable put down in every way that truly matters, and a reasonable put down precisely a reasonable set out some reasonable set out some reasonable compromise. The need for remote data protection was met by the unexpectedly high number of workers who were compelled to work from home due to the coronavirus outbreak. Wherever employees who unfortunately had to use their personal laptops, there the risk gets heightened as personal laptops carry many other personal data apart from the company's confidential data, thus this demands for adhering to business standards to ensure the data is protected in work from home mode. Apart from this as there exists a different type of SMBs sectors in Oman, ranging from tourism and hospitality, food and beverage, retail, technology, IT services etc thus data protection has become crucial for the SMBs in Oman. Also with the increased cloud computing, e-commerce, and digital payments, protecting customer and business data has served as an important role in preventing cyber threats, data breaches, and financial losses. Thus, prioritizing data protection can empower SMBs in Oman to embrace digital transformation confidently and will also equip them with ways to mitigate risks and maintain a competitive edge in a growing digital economy.

There are various data protection techniques that the businesses employ in order to protect all the confidential data related to their employees, customers and company's protocols depending on the nature of the business type or sectors from which the SMBs belong. Most commonly the business opts for two options as their data protection techniques one is tape and other one is disc-based system. In a tape-based technique it empowers the company to take backup of the data and moves the data to a tape cartridge or disk-based storage array. A good option for data security against cyber-attacks is tape-based backup. Tapes might be sluggish to access, but they are often detached and adaptable

when not stacked in a drive, making them safe from network attacks. In some cases, businesses also use the technique mirroring to make a precise copy of a website or data so that it can be accessed from anywhere in the world. In addition to this, companies also leverage Continuous Data Protection (CDP), this empowers the companies to back up all of the data in an organisation whenever change is made, thus this empowers companies for speedier data recovery.In addition to this, monitoring and making data accessible are the fundamental principles of data protection. The concept of "data protection" encompasses both operational data assistance and business continuity/disaster recovery (BCDR). Data management and data availability are the two main axes around which data protection systems are built.

Whether the data is damaged or deleted, data availability guarantees that clients have the information they need to run their businesses. Data lifecycle management and information lifecycle management are the two fundamental categories of data management utilised in data security.

A technology called data lifecycle management automates the improvement of basic data for offline and online storage. A comprehensive method for tracking, predicting, and safeguarding information assets against software and human failures, malware and virus assaults, hardware malfunctions, and facility power outages and disturbances is information lifecycle management (Habibzadeh et al. 2019). Recently, data management has broadened to encompass figuring out how to control, govern, and guide the initial business benefit that comes from using data for analytics, test/dev enablement, and other objectives without giving it any thought.

According to Alkhattali (2025), the adoption of digital integration by the companies in Arab countries including Oman has empowered the companies in multifaceted ways particularly in streamlining operations and also in enhancing competitiveness. On the other hand, the integration of the digital technologies enables companies with automation, effective resource optimisation and cost reduction scopes thus ultimately improving business efficiency. But the study has highlighted that the transformation of digital technology has introduced the company with several data

protection challenges, particularly in cyber security vulnerabilities, compliance issues, and organisational resistance to change. The study has highlighted that with the help of the digital technologies companies got an opportunity to get global access thus allowing them to improve Customer Relationship Management (CRM), but the threat of cyber security and data breaches has remained unaltered. And this happens due to limited digital skills and high implementation costs thus further hindering SMEs from adopting data protection measures. Protecting data in this digital era has not become a necessity for the companies but it is considered as a strategic move for the SMEs in Oman to achieve long term sustainability, innovation and competitiveness in the rapidly evolving digital economy.

In comparison to this another study by Morshed and Khrais (2025), has highlighted that the rapid digitalization in the Arab Gulf Region has been made possible due to the Saudi Vision 2030 and the UAE's Smart Government strategy. This has accelerated the integration of advanced technologies into the accounting process. With the help of this digital transformation, Business Intelligence and Enterprise Resource Planning (ERP) systems have enhanced efficiency and also allowed businesses to enhance their decision-making ability. Although this has empowered the businesses to enhance their decision-making powers, at the time companies were exposed to cyber security threats, including phishing, ransomware, and insider attacks. Thus, the study has highlighted the significance of robust cyber security practices, ethical accountability, and regulatory frameworks in securing digital accounting systems. The study has been conducted with the help of a quantitative research approach and has highlighted that with AI driven threat detection with an effective and tailored employee training method this can significantly improve trust upon the companies. Apart from this adhering to ethical standards also mediates these effects. Thus, the findings suggest the necessity of developing integrated cyber security strategies that combine technology, ethics, and compliance for the SMBs in Oman. Organising training programs, AI-powered threat detection and adhering to ethical standards strengthen resilience against data breaches.

2.3.2.2. Challenges faced by SMBs in the Oman in managing data

Business worldwide has emphasised on data which has been a valuable asset for the organisations which enables them to make better decisions and help them gain competitive advantage. Despite various benefits of digital transformation within SMBs in Oman, this has also resulted in posing several significant threats related to data. This further results in hindering the ability of the organisation in harnessing the full potential of their data. Some of the significant challenges that SMBs, particularly related to data, are restricted resources because of constrained budgets due to which SMBs mostly face issues in investing into the sophisticated data analytics tools. Additionally, this also results in working as an obstacle for the implementation of advanced data infrastructure due to which it becomes difficult for SMBs to make data-driven decisions. With increased reliance on digital transformation, SMBs face large issues of data privacy and security which needs to be addressed effectively. Failing to do so can result in affecting the business operations negatively. Issues in data protection and security not only affects the business negatively but it also results in eroding the trust of customers. Customers are unaware of how their personal data and information is managed within SMBs which highlights lack of transparency within the business operations.

Another significant issue related to data protection management focuses on navigating the policies, laws, and regulations based on data protection, making the business environment quite complex and dynamic for the customers. The privacy of data is often considered a highly complex area that is underfunded and understaffed, further requiring the SMBs to enforce effective policies while offering employees to attend proper training sessions to address inadequate data protection systems. Technology disruptions also result in the issues of data privacy. With evolving digital technology, the protection of data has become quite complex for SMBs. Additionally, these complexities further lead to increase the potential for human error further resulting in security threats from the cybercriminals when using the same technology that is being used in the SMBs.

Data leak or breach is one of the most common events of data security that occurs within organisations which results in disclosing the personal information of the customers to unauthorized viewers. These can occur within SMBs because of several reasons including cyberattacks by external advertisers, data theft by employees, partners, or contractors, loss or theft of devices with important personal information, and human errors by sending sensitive information to wrong recipients accidentally or mistakenly. This results in affecting the financial impact of the organisation causing reduced revenue, increased legal costs, damaging customer trust, and compliance fines. A study by Olawunmi (2020) emphasised on understanding the issues related to data privacy and GDPR in Irish SMBs. The study emphasised on integrating GDPR framework to address the issues of data breaches and hence mandated SMBs to adopt significant policies and guidelines within the business operations so that the organisation regulates the data and store it safely and securely. Another study by Maroufkhani et al., (2020), SMBs have largely adopted big data analytics to enhance their performance. The study determined the mediation impact of BDA to understand the association between the environmental, organisational, and technological contexts along with the performance of SMEs. However, the issues in the financial and marketing aspects of the SMEs have been determined as challenging which needs to be improved.

Various digital technologies have been largely utilised within SMBs in Oman. One of the most common technologies is Cloud computing which offers opportunities as well as poses threat to the customer's data and risks. The COVID-19 epidemic has changed how companies operate. As more employees utilise conferencing and collaboration services while working from home, it is putting a strain on back-end support systems and increasing traffic on networks that link users to these services. The extra demand will only be supported by service providers with sufficient architecture and a steady quality of customer service.

Cloud providers often have difficulties with their business continuity strategies. They have to answer difficult questions like whether their public cloud architecture can continue to deliver services even in the event that support staff members fall ill and if it is

robust and scalable enough to handle growing demand. They must consistently demonstrate that the underlying infrastructure is robust enough to ensure continuous access to public cloud services and that the network infrastructure can handle increasing traffic volumes. To do this, however, cloud providers need to understand the risks, opportunities, and events that might occur due to the pandemic. They need to demonstrate that they can handle unexpected spikes in demand (Mandal and Khan, 2020).

However, businesses also have the opportunity to demonstrate how the steep and quick increase in the number of people working from home has tested the flexibility and resilience of their services. Cloud service providers must be aware of the challenges posed by the increase in demand. The already high demand will be further exacerbated by remote work, streaming services, and the substitution of digital events for in-person meetings. Operating support for cloud solutions will need to be maintained while working remotely or with fewer staff members since manufacturing facilities are based in China and other areas impacted by the current events. Supply networks will be impacted by shortages as well. Cloud services provide that Cloud service offers that haven't undergone stress testing could not be equipped to handle these dangers.

Another major issue for data protection and security is ransomware which results in affecting the SMBs adversely. This type of virus, which keeps data hostage in exchange for money, is becoming more and more common. Data protection against ransomware has been accomplished using conventional backup techniques. Nevertheless, increasingly advanced ransomware is adapting to and avoiding conventional backup procedures (Doyle et al. 2020). After some time, the most recent iteration of the malware gradually gains access to an association's data; as a result, the association ends up backing up both the data and the ransomware virus.

It is difficult, if not impossible, in this circumstance to return to the optimal form of the data. In order to address this issue, vendors are managing to modify backup and recovery products and processes in order to interfere with the new ransomware capabilities. Additionally, companies must take reasonable precautions to protect the data they keep

because ransomware risks are increased when employees are less protected and when they use insecure networks.

The number of copies of data that an organisation needs preserve is reduced by CDM, lowering the amount of data that must be stored, managed, and protected. Through automation and centralised control, CDM may shorten the time between application release cycles, boost output, and reduce administrative expenses.

The next phase of CDM is to incorporate additional intelligence. Businesses like Veritas Technologies integrate CDM with their complex data management solutions.

2.3.2.3. Gaps in Data security and technical progress

As SMBs in Oman are rapidly undergoing digital transformation, adopting advanced technologies to enhance efficiency and competitiveness. However, this transition is presenting unique challenges for the companies which they are not familiar with. Thus, despite the global advancements and introduction of AI, other advanced technologies and advancements in cyber security and data management, many Omani SMBs struggle to implement robust security measures and keep pace with evolving technological demands.

Overtime with the rapid digital transformation, data security has become a critical concern for every Omani SMBs, yet many enterprises lack the necessary infrastructure, policies, and expertise to protect sensitive information, thus highlighting major gaps in the data security systems and thus indirectly affecting their technical progress.

In the post COVID-19 period, cyber threats have escalated in the GCC, exposing SMEs to face financial instability and operational risks. The study by Webb and Sallos (2024) has highlighted that the SMEs in Oman are susceptible to the cyber threats because of the gaps in data security and inadequate technological advancements in managing data. The study emphasizes the importance of advanced detection systems, enterprise-wide security strategies, and regulatory frameworks to mitigate these threats.

Alsoin order to address such types of risk there shows a need for continuous

monitoring, and this further allows for mitigating cyber security risks. Continuous monitoring equips companies with innovative and scalable solutions that are not only effective for mitigating such risk but also offers tailored solutions for the SMEs who are undergoing digital transformation. Thus, the study has highlighted proactive strategies that equip Omani FinTech SMEs with the necessary tools to strengthen cyber security, safeguard operations, and enhance data protection in an evolving digital landscape.

One of the primary reasons for gaps in data security is due to the absence of dedicated IT security teams who have hands-on experience, and their expertise allows them to reduce and mitigate these risks. But due to this majority of the companies are exposed to vulnerable cyber threats in the post COVID-19 period. As SMBs are restricted with financial constraints this does not allow them to hire an expert IT team who can support them in crisis and thus resulting in an increase of data breaches through phishing attacks, ransom malware etc. As propounded by Heidt et al. (2019), has examined the security gap between SMEs and Large enterprises. It has been found that the SMEs are lagging due to inability to invest in IT security teams for the SMEs. The study has highlighted that factors that the SMEs are lacking are skilled personnel, structured processes, and planned IT budgets. And thus, this has highlighted the need for a strategic approach that can effectively bridge the security gap between the SMEs and Large enterprises.

In contrast to this a study by Chitra *et al*., 2025 has highlighted the role of cloud computing in addressing the challenges faced by the SMEs. The study has highlighted how cloud adoption enhances SMEs' global economic contributions by providing cost-effective, scalable, and secure solutions. Cloud computing offers SMEs pay-as-you-go access to enterprise-grade technology, enabling remote collaboration and operational flexibility. But the study has highlighted that security, efficiency, and scalability factors influence companies to adopt cloud computing. In addition to this the study has also highlighted that offering effective training to the employees or work force may empower the company to have strong data security which can further ensure them with robust

backup and recovery procedures. In comparison to this another study by Tejada, 2020, has highlighted the impact of technology on SMBs, and thus emphasizes how the digital solutions empower SMEs to stay competitive. The rise of the (IoT) and increased cyber threats have made SMBs prime targets for cyber criminals. This study has also highlighted that the cyber threats have increased due to limited resources, insufficient security budgets, a lack of trained personnel, and inadequate awareness of cyber risk exposure.

A study by Chidukwani et al. (2022) has highlighted that SMBs face cyber security threats due to inadequate cybersecurity measures. Despite their economic importance it shows that the SMBs do not adopt effective security measures and a demand for improving and implementing these measures is essential to mitigate the cyber threats.

Mitigating these cybersecurity risks depends on an integrated strategy that considers cost efficiency and security measures. One of the major solutions involves the deployment of security-as-a-service (SECaaS), where SMBs are easily able to secure high-level security for their organizations especially because they do not need to have enormous investment or human resources in this area. Outsourced cybersecurity providers are also likely to have access to current threat intelligence, carrying out monitoring continuously, or providing incidents frequently. Moreover, the government programs aimed at providing cybersecurity grants and offering training possibilities for SMBs can contribute to the reshaping of the latter's knowledge of current threats. Besides, external security solutions, it is vital for SMBs to develop a security culture within their organization. This can be done by providing multi-factor authentication, updating the software, and encrypting the data to minimize cyber security threats. In addition to this, AI-based security tools will help in identifying threats as well as responding to security threats since AI solutions can be integrated to automate the processes of detecting security threats. This increases the importance of planning and investing in SMB's security strategy since the above-made strategies can only work

where SMBs are willing to shift away from purely reactive measures. Hence, whether the Omani SMBs are ready and capable of coping with the dynamic threats that emanate from the increasing digitalization in the business world will define the level of sustainability and competitiveness of these firms in the consolidated business world (Chitra et al., 2025).

2.3.3. Recommendations assisting in the reduction of cybersecurity issues in SMBs

2.3.3.1. Strategies to recover from digital disaster

The outbreak has brought attention to the existing digital divide among countries, even if there is still much space for digital development. Due to their failure to maintain essential enablers like reliable and affordable Internet connectivity, certain low-pay nations have been abandoned as high-pay countries have increased their embrace of digital technology. These low-wage nations will face greater disadvantages as an outcome of the Coronavirus-driven digital transformation initiatives.

As more devices and systems are connected to the Internet, they are unable to take use of technology, It makes the unequal distribution of benefits from the digital economy even worse. To guarantee that all individuals have access to digital technology and that emerging nations may equitably benefit from the digital economy, it will be necessary to make fundamental investments in broadband infrastructure.

Digital technologies are widely seen as an effective way to advance equality in a number of areas, including access to healthcare, the job market, and education. Due to social distance requirements, other Coronavirus-related regulations imposed by governments starting on one side of the world then moving onto the next, and shifting consumer interest throughout the pandemic, the Coronavirus crisis has sped up digitalisation processes in the two services and assembly in the majority of countries, though at varying speeds.

Women have been negatively impacted by the coronavirus pandemic as an outcome of the increased dangers to their financial security and likelihood of losing their jobs, in addition to the strain of caring for their families and providing thought during the

lockdown. We look into some of the lessons discovered regarding the pandemic's effects on gender equality as well as how far the digital transformation could actually benefit women overall.

As seen in the new construction and expansion of digital infrastructure, the shift to digital transport of services by businesses and inside organisations, such as in education, clinical consideration, and retail, and increased execution of digital technologies in assembly. The coronavirus crisis has accelerated the trends in digital transformation starting with one side of the world then onto the going with. Despite the fact that the epidemic has negatively affected many enterprises, it has also made fresh chances for entrepreneurship apparent.

For example, it has increased digital entrepreneurship, reflecting the shift in consumer behaviour caused by the epidemic and its effects. Because it has had a negative effect on women in the majority of countries, the recession linked to the Coronavirus epidemic is sometimes referred to as a "shecession." Although the pandemic has mostly harmed women, it has also highlighted previously ignored direction prejudices, such as the direction racial-gap, that have previously only affected males.

When considering the danger to prosperity, for example, we see that Black women in the US are defenceless and more likely to contract the Coronavirus than Black males or White women. The authors attribute this to the increased risk of sickness that Black women face in low-wage occupations in sectors that provide important services, such as healthcare, transportation, and warehousing, where they are overrepresented and where remote work is not permitted. Black women have always worked in risky jobs (Schiuma, 2021).

The adoption of Industry 4.0 technology is a paradigm that was at that point clear before the pandemic experience and as would be expected usual to intensify in the post-pandemic period. In the wake of the pandemic, the role of Industry 4.0 technologies in achieving resilience has become even more fundamental, with 90% of assembly and supply chain specialists expressing a willingness to invest in digital capability. Regardless of an association's current technology infrastructure, adoption of some Industry 4.0 technologies, like the use of the industrial Internet of Things or operator

assistance through expanded reality in digital execution management, should be evident without significant technology investments.

Workers who do duties that can be replaced or changed by employing Industry 4.0 technologies will likely be impacted by the faster adoption of these technologies. While some Industry 4.0 technologies may replace jobs, others will increase worker productivity or improve workplace safety. Regarding how digital technologies affect workers' occupations, there are clear direction gaps of considerable size. Women in emerging and transitioning economies are much less likely than males to have the standard skills—specifically, scientific, non-routine manual, interpersonal, advanced ICT, and socio-local skills—that might protect them against the negative consequences of digitisation. As more solutions become available and costs fall down, Disaster Recovery as a Service (DRaaS) is becoming more and more popular. These days, DRaaS is used for critical business systems where data is being duplicated instead of just backed up.

Digitization involves converting traditional paper-based processes into digital formats to enable computer-assisted information management. In contrast, digitalization is "the sociotechnical process of using digitized products or systems to create new organizational practices, business models, or commercial offerings." This means that digitalization encompasses the partial or complete transformation of business models and activities along the value chain into digital platforms, using technologies including block chain, artificial intelligence (AI), mobile and visual interfaces, cloud computing, robots, smartphones, additive manufacturing, 3D printing, and the Internet of Things (IoT).

Innovative solutions or well-integrated digital platforms can bring about such a change. Businesses may successfully cooperate on research and development and take advantage of new market possibilities with the use of tools like websites, social media, cellphones, content-sharing platforms, e-commerce systems, blockchain, automation technologies, robots, and wearable technology. Although many firms have not yet completely embraced these technologies, the COVID-19 epidemic has sped up their implementation.

Research indicates that digitalization is driven by factors such as the increasing pace of innovation, new forms of consumer accountability, and enhanced business process efficiency. To capitalize on market opportunities, businesses need to initiate and expand the use of digital technologies in ways that enhance value-adding activities. This process, known as "business-model innovation," involves discovering "new ways to generate revenue and define value propositions for customers, suppliers, and partners," with a primary focus on finding innovative revenue streams for the business.

Businesses may grow more entrepreneurial as environments get hostile, but only up until a point where the intensity of the obstacles drives them to switch to a general defensive posture. According to recent research, these concerned natural factors may include price wars, pandemics, fluctuations in commodity prices, recessions or depressions, or significant changes in governmental policies and political ideologies. Brilliantly low business risks (harmless environment) and fantastically huge business hazards are the two extremes. Nevertheless, the potential presented by digital technologies and the internet for organisations to redesign their business models have been constrained by factors like as organisational firmness, the digital divide, and the unequal impacts on worker prosperity. Availability of user-friendly digital technologies, reduced costs for digital data storage and the potential proficiency gains that could arise from this, the cost savings and improved time management that come with working from home, and the potential for flexibility.

Thus, in addition to descriptions of the digitisation of marketing, transportation, supply chains, and retail, the report highlights the digitalisation of office labour. Organisational resoluteness and conviction systems exist concurrently because transitions towards the digital office are hampered by smaller organisations, cash-based business practices, and the digital divide between the haves and have-nots. This research conceptually contributes to the existing debate on coronavirus by analysing the transition and processes towards digitisation by companies, focussing on the internal factors, people, and work, and tracking this in a more undeniably near, to setting.

Realistically speaking, our data supported the argument that despite the recession, firms may still adopt some features of digitalisation. This could be a potent tactic to combat difficulties and help businesses come out of the crisis stronger. Our data also supports the idea that businesses must re-evaluate themselves or run the danger of becoming the victims of a competitive market. Given the observational data from business failure research, which has demonstrated that one of the primary reasons of business failure is the incapacity to modify the firm's services and business model in response to changes in the external environment, this is evident.

Our analysis highlights the need for governments to establish financial incentives and policies that facilitate firms' transition to profit from digitisation, while also speaking to the ongoing strategy of digitalisation, starting with one side of the world and working forward. Thus, it has become increasingly clear that governments should concentrate on developing and expanding technology infrastructure to further promote access and provide traditional communities with the new digital economy.

Government resources are required to build a technological infrastructure that gives new and developing enterprises the foundational support they need to take advantage of and make the transition to new technologies, which is especially important given the circumstance that is creating it. For instance, governments may grant small enterprises financial aid or technology gadgets. This might increase openness in corporate operations and aid in the application of cost and productivity standards.

Additionally, the adoption of new technology typically revolves on business objectives. It is true that when businesses adopt powerful new technologies all of a sudden, productivity frequently suffers in the short- and long-term; This would greatly improve corporate processes and efficiency if employees in faraway locations put out a reasonable amount of effort. Additionally, there's a risk that using technology during this crisis might lead to a greater "psychological dividend." This is where a lot of individuals, including managers, employees, and customers, have been compelled by the pandemic to embrace technology that they had previously shunned. It is also possible, when considering the more fundamentally plausible ramifications of the observations made here, that employers would

try to lower the pay of workers performing tasks from unimportantly expensive locations and unimportantly expensive non-industrial countries.

Automation is the main effectiveness strategy. With automation initiatives, the return on investment is almost immediately apparent, balancing the simple outlay. Organisations can automate specific work processes using mechanical process automation to save time on expensive manual tasks and reallocate resources to other areas of the business. The economics of automation are straightforward: the same work is completed more quickly and accurately, and HR can be redeployed to higher-value tasks or fill in for basic deficiencies. Foreseen waste areas can be identified, and they can be addressed using more advanced machine learning tools.

Holding governments responsible is a crucial function of normal society if they are not always trusted to act wisely or in the best interests of outside businesses and society at large. NGOs are still vital in helping SMEs acquire digital skills, but promoting informed digitisation also requires raising awareness of the benefits and risks that digitalisation presents to SMEs and society as a whole.

Crisis situations are the perfect times to double down on digital transformation, regardless matter how irrational they may appear. Organisations should take all the risks necessary to implement digital transformation strategies rather than necessitating their postponement. The price should not be prohibitively high. Given the current climate of uncertainty, many firms are naturally reluctant to relax their financial restrictions. Digital transformation should not be viewed as a significant direct investment in results with increased duration. Some of the most successful transformation initiatives start with little funding and low-cost experiments. which are then scaled up after the kinks are ironed out and the results are proven. When done correctly, digital transformation can support itself, with each steady advancement covering the cost of the subsequent leg of the journey.

Beyond its immediate economic implications, the pandemic is probably going to have long-term repercussions, such significant disruptions to business operations and tourism-related industries. Technologies can assist to lessen these economic repercussions by allowing businesses to access customers digitally, continue to operate

while utilising remote working arrangements, and overcome logistical challenges caused by disruptions to global supply networks. Evidently, it is projected that in Malaysia, technological solutions that lessen the risks that the coronavirus offers to organisations might provide a sizable 72% of the economic value that could be achieved by adopting emerging digital technologies.

In the post-pandemic era, digital technology will remain essential for improving the resilience and competitiveness of businesses. Governments may accelerate efforts to transition to the digital age by increasing their regulatory, financial, and advising assistance for companies, particularly micro, small, and medium-sized enterprises (MSMEs) that lack digital competence. This might include extending access to high-speed Internet and broadband infrastructure, as well as offering incentives and guidance to firms on digitalisation.

The global coronavirus pandemic has drastically affected consumer behaviour and increased electronic sales since coronavirus limitations have a negative influence on foot traffic in conventional physical retail outlets. By 2020, the value of international business-to-consumer (B2C) sales in the Asia-Pacific region was estimated to be $476 billion, or 31% of all B2C online company sales in the region. For MSMEs, this presents a big potential since it allows for the promotion of foreign trade at far lower prices than in the past (Schiuma, 2021).

Nevertheless, enterprises must overcome a number of obstacles to engage in internet commerce. MSMEs most commonly face two types of barriers: financial and regulatory. These include the substantial customs duties levied on new electronic trade, the high costs of cross-border logistics, and the stringent consumer protection regulations in other countries. To assist MSMEs in overcoming these obstacles, governments may use a variety of strategies, including offering incentives for internet-based businesses and products as well as training on new rules. The epidemic has sped up the rate of digital adoption in their firms, according to 87% of respondents. There is a shortage of digital skills, and present training initiatives are unable to keep up with the growing demand for these talents. Only 30% of firms that see the need for training their employees in digital

skills have completed a strategy to do so. A fundamental problem that requires immediate attention is the lack of digital skills. There is little doubt that even once the epidemic is over, there will still be a significant need for digital technology.

According to a World Economic Forum research, employment changes are occurring more quickly than in the past due to the shorter development cycles of artificial intelligence and other developing technologies. Employees should engage in digital skills training much more frequently to remain on top of the quickly changing work requirements as new positions are created and skill requirements increase.

In order to unlock the potential of their future workforce, it is critical that governments and corporations remove these training impediments. Offering financial assistance for workplace training in digital skills. They might engage in actions like promoting industry-driven training programs and establishing public-private partnerships to increase awareness of the benefits of training.

2.3.3.2. Strategic Planning for cyber threats

ERP systems automate planning, inventory control, and other corporate operations. They are computer-based tools for managing and organising information flows both internally and externally, from HR and materials to finance and sales.

Technologies for radio frequency identification (RFID) aid in redesigning logistics and manufacturing efficiency. Close-range communication is made possible by RFID technologies, which are utilised for applications such as installation, access control, supply chain and inventory tracking, as well as for applications such as product identification, person identification, and production monitoring and control. Additionally, front office integration and supply chain operations are aided by software for customer relationship management (CRM) and supply chain management (SCM). The management is of an association's contacts with its members, clients, prospects, staff, and suppliers using CRM and SCM software.

Cloud computing enables the upgrading of IT infrastructure. Cloud computing (CC) is the term used to describe ICT services that are available over the Internet, including servers, storage, network components, and software applications. CC gives

SMEs the chance to access databases, software, and additional processing or storage capacity online in amounts that match and adhere to their demands. Despite its adaptability and scalability, CC lowers the cost of technology redesign by relieving businesses of open hardware investments and customary costs for maintenance, an IT team, and check. It should go without saying that businesses adopting an ICT management style that is more focused on software acquisition and digital networks are linked to both greater cloud computing adoption rates and lower levels of ICT expenditure in equipment.

Big data analytics may be applied in many different ways inside the organisation to increase productivity in marketing, advertising, and commercialisation, as well as in general administration, manufacturing, pre-production, logistics, and strategic planning and decision-making. “Data analytics” describes the use of techniques, instruments, and software to analyse vast amounts of data produced by electronic and machine-to-machine interactions.

Social media helps SMEs grow their consumer base, brand awareness, and activity. Social media is mostly used for external interactions, such as promoting businesses' reputations, selling items, and soliciting or answering customer feedback, reviews, and inquiries. Social networking may also be used to choose staff or business partners. Online businesses help SMEs expand their client and supplier bases and enter markets outside of their conventional geographic borders. Online business refers to the sale or acquisition of products or services made through PC networks using procedures intended only for placing orders. E-orders and e-booking are more sophisticated variations on e-sales. A wide range of different commercial ties, including any potential alliances between consumers, companies, or governments, is used in electronic commerce (Artemieva et al. 2019).

These include business-to-business (B2B) and business-to-government (B2G) transactions, which together still account for the majority of private sector electronic business turnover (for instance government obtaining). Consumers are becoming more directly involved in online commercial transactions, particularly sales from business to

consumer (B2C). Peer-to-peer and consumer-to-business (C2B) interactions, which occur between two or more individuals, are also a part of emerging business models. B2G applications encourage SMEs to adopt more technology while lowering administrative burdens and, surprisingly, the likelihood of government-SMEs interactions.

Electronic invoicing encourages consistency via design strategies, enables the integration of accounting software and expenditure guidelines, and eventually shifts the burden of administrative burden to SMEs. The transmission of pay-as-you-secure arrangements for business keeping and responding to regulatory authorities, as well as safer information chains between organisations and the execution of company strategies, are all supported by electronic invoicing. The management of instance charges is taken into account by e-invoicing systems to go beyond individual yearly assessment forms, (completely) pre-fill corporate yearly responsibility and value-added government forms.

High-speed internet is a requirement for the digital transformation of SMEs. High-speed fixed broadband is defined in this article as having a download speed of around 100 Mbit/s. For existing Internet services to be fully utilised and for the spread of new ones, a satisfactory network connection speed is necessary. Customers notice differences in speed levels significantly. High-speed broadband users, for example, may download a 1.5 GB high-quality movie in less than 22 minutes, whereas low-speed users have to wait about 52 minutes to do the same work.

Thus, various business ICT usage indicators may be used to track the digitalisation of some SME business processes much more precisely. SME use of digital technologies is subpar across the board. With regard to large companies, the difference in SME diffusion rates is a constant across all technologies for which statistics are available. Small businesses continue to be less digitally savvy than medium-sized businesses, who in turn are less so than big businesses.

In all honesty, trends across small, medium-sized, and massive enterprises are relatively similar, with the larger just going down the diffusion spiral quicker. As a last option, SMEs will digitalise their marketing and general administrative processes first. The prevalence of B2G interactions does not significantly differ between small, medium-

sized, and large businesses. SME adoption rates are higher for supply-customer management software or social media. When using electronic invoicing or engaging in online business, the gaps between different firm sizes are also narrower.

When technologies advance or reach a wider audience, the gap in adoption widens. ERP systems are especially less common in small enterprises than in large organisations. ERP systems are used by companies that are large enough to handle the unpredictability of ERP implementation and the significant time, financial, and reskilling resources needed. Consequently, the ERP diffusion gap among small and medium-sized enterprises is significantly greater than that of big and medium-sized enterprises (Artemieva et al. 2019). When it comes to SCM software or big data analytics, the digital gap between medium-sized and large businesses grows. However, large corporations have made far greater investments in integrating their business processes, strategic planning tools, and production and logistics management software.

To combine their IT systems, many corporations are turning to external CC services. Businesses often prioritise storage space and email services above office application access and database hosting. This is true for both small and large organisations, although larger companies have been more aggressive than smaller ones in externalising new IT system development and maintenance.

Story certification implies that a digitalisation process is underway even among micro-firm personnel, even if it is still challenging to appreciate its scope and understand its details without particular data. The majority of enterprises have some kind of online presence through social media platforms rather than a website, according to a 2015 covert poll on small businesses with less than five workers in Australia, Brazil, Canada, India, Turkey, the United Kingdom, and the United States. These businesses had tiny representative cash bases and little clientele, which decreased the section cost of website ownership. Of those surveyed, 22% have no electronic presence at all. According to a recent survey by the European Investment Bank, 80% of large companies have adopted at least one digital technology, whereas less than 30% of microbusinesses have done so.

It is possible to draw conclusions about the digitisation of microbusinesses from trends on digital platforms. Without a doubt, new electronic business models backed by online retailers such as Amazon provide small businesses an unprecedented opportunity to increase their customer base and income, get economies of scale through network effects, and pay very little for business intelligence services. On the plus side, digital platforms may assist microbusinesses in cutting expenses and boosting efficiency in a variety of company operations, such as marketing, sourcing, innovation, support, and more. Because they are usually more agile and adaptive than bigger companies, micro-firms might make the transition to digital platforms and these new business models much more quickly.

2.4. Summary of Literature Review

This comprehensive review of the academic literature and existing peer-reviewed studies have discovered undiscovered insights, views, and gaps across the research domains that are relevant to focus when identifying the answers to the research questions. Based on this, the actual findings of the studies are summarized below which highlight the current understanding and limitations to carry out further investigation.

The review of the existing literature on highly advanced digital protection and security with the implementation of digital transformation during COVID-19 highlighted remarkable shift in the SMBs. The shift from traditional methods to digital tools resulted in offering benefits to the SMBs. Due to increased benefits, SMBs largely adopted digital transformation as going digital was the only way left for businesses to operate, especially during the difficult times of the Coronavirus outbreak. As the pandemic has led to the vast adoption of digital platforms within SMBs, it has also resulted in data protection and security issues that has caused the business to adopt significant strategies to deal with these data-related issues.

SMBs have largely relied on adopting digital technologies such as AI-powered technologies, IoT devices, big data analytics, and cloud computing. These advanced technologies offer businesses with enormous opportunities and benefits that are also an

important part of the economy by contributing in the GDP and increasing employability. Despite this, the increased adoption has led to issues related to data stored by organisations through online transactions, digital engagement, and mobile applications. The literature further discusses data-related issues including digital vulnerabilities, threats to data protection, recent challenges faced by SMBs, recent attacks, and steps taken by attackers, phishing attacks, malware attacks, and ransomware. This helps determine the impact of digital transformation on the issues related to data, especially in SMBs.

Furthermore, the adoption of digital platforms within SMBs resulted in providing the potential to improve their productivity, creativity, better and informed decision-making, and offering customers with better experiences. However, customers also have trust issues with the implementation and deployment of these technologies. SMBs mainly face issues related to data which further results in creating trust issues among the customers about the protection and security of data they shared with the business. Focusing on this aspect, the increased need for data protection and security was considered reasonable. The increased significance on data protection resulted in ensuring the security of data, and protecting data by putting down in an appropriate manner. In addition, significant challenges such as digital disruptions, data breach, issues of data security, strained back-end support systems in cloud computing has resulted in affecting the SMBs negatively. Nonetheless, gaps in data security and technical progress have also been identified within Omani SMBs because of lack of infrastructure, effective policies, and expertise in protecting sensitive data. Along with this, financial instability and operational risks are also determined as major gaps that affect the technical progress of the technology and issues in data security.

Lastly, significant recommendations have been determined to understand the effective strategies that are important for SMBs to recover and fight against the disaster that happens due to the adoption of advanced technology. Effective strategies thus, help SMBs in gaining the trust of their customers by safeguarding the data provided by the customers and storing them adequately. Not only this, but when the strategies are adopted

by the SMBs, it also contributes to the economy by enhancing its GDP growth rate. In addition, strategic planning for addressing cyber threats within ERP systems have been discussed to corporate operations. RFID, ICT services, and social media are some of the ways that help SMBs to gain a large consumer base and stay competitive.

2.5. Gaps in Literature Review

The extensive analysis of the literature has revealed critical gaps in the implementation of digital transformation and the protection and security of data, especially in SMBs within the context of the Sultanate of Oman. As digital technologies have been largely focused upon, several directions are still there that are yet to be explored. The critical gap in the literature indicated the lack of empirical research on understanding the impact of digital transformation on small and medium-sized businesses with a focus on data-related issues. As the study has been conducted in Oman, it emphasizes on determining the impact of digital transformation and data-related issues in Omani SMBs. However, the literature review lacks proper information on data protection and security within SMBs in Omani context.

Further, the literature has also revealed lack of studies with a focus on technical progress as compared to the studies related to inadequate security. As the study further focused upon identifying the data-related issues including inadequate security and technical progress, the literature search did not found studies involving SMBs management that result in affecting the technical progress and data security with the shift towards digital transformation. The literature search has determined studies that have involved digital technologies such as cloud computing indicating challenges faced by the management of the organization, however, the literature found a gap, especially in determining the challenges that hinder the technical progress of digital technology, especially within Omani SMBs management.

At last, the study focused on recommending significant strategies that are considered effective for minimizing cyber threats after the implementation of digital technologies within Omani SMBs, however, the literature determined a knowledge gap in finding studies that mainly focused on issues related cybersecurity in SMBs within the

Omani context. Various studies have been determined focusing on the strategies to safeguard data protection, however, no studies have explored about cybersecurity within Omani SMBs. Thus, the literature has involved studies that has focused on addressing cyber threats in SMBs in countries other than Oman.

Table 2.1: Gaps in the Literature

Author (s)	Title of the study	Findings	Gaps Identified
Bisht and Singh (2020)	Challenges faced by micro, small and medium enterprises: a systematic review	Businesses earn lowered revenues because of restricted infrastructure and financial constraints	Did not focus upon SMBs within the Omani context.
Busaidi et al., (2022)	How can small and medium enterprises create employment opportunities: case study on Oman	SMBs have largely adopted digital transformation that further boosts the economy	Lack of focus on data-related issues with the adoption of digital tools.
Morshed and Khrais (2025)	Cybersecurity in digital accounting Systems: Challenges and solutions in the Arab Gulf region	Challenges related to phishing attacks, ransomware, and cyberattacks have been determined	The study did not emphasis on Oman.
Olawunmi (2020)	GDPR & Data Privacy: Impact of Data Protection in Irish Small and Medium-Sized Enterprises (SMEs)	Issues related to data privacy and security have been identified in Irish SMBs.	The study did not focus on Oman.
Artemieva et al., (2019)	Challenges and Opportunities of Digital	Potential alliances between consumers, government, or	The study did not focus on SMBs in Oman.

	Transformations in the Economy	companies are helpful for e-commerce business	

2.6. Conceptual Framework

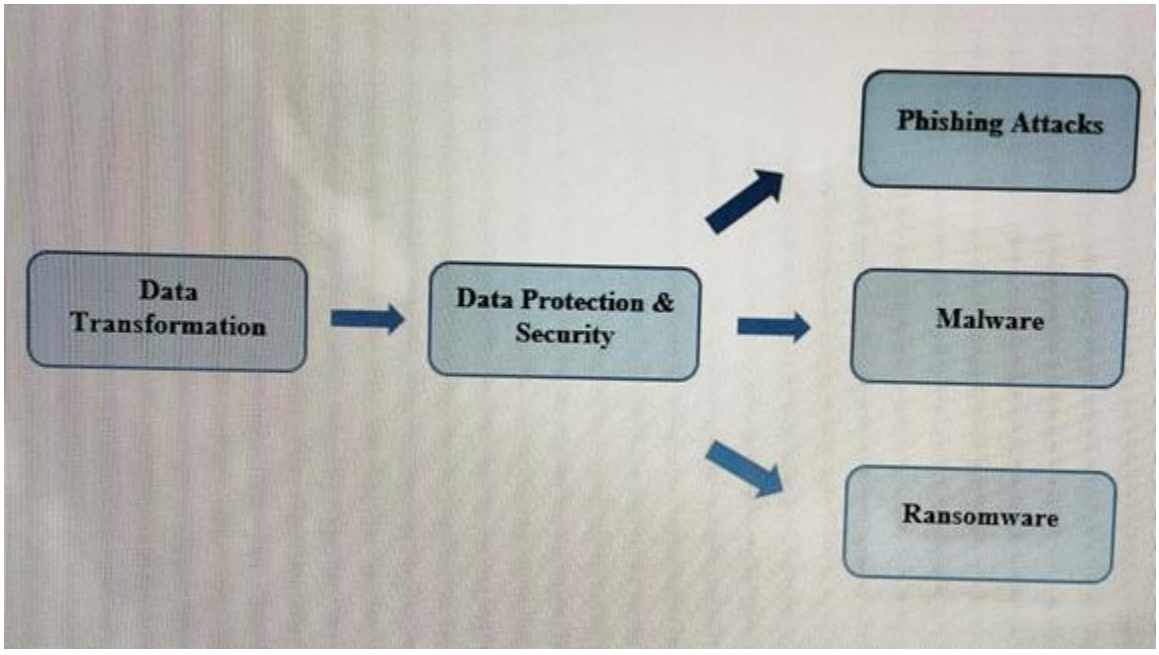


Figure 2.3: Conceptual Framework

Based on the valuable insights determined through literature review, the conceptual framework emphasizes on determining the impact of digital transformation based on data-related issues in Omani SMBs. The extensive literature review revealed knowledge gaps regarding the implementation of cybersecurity threats, data protection, and technical progress within Omani SMBs context. Thus, the framework emphasizes on determining the connections between the dependent and independent variables based on the research context.

The conceptual framework emphasizes on mapping the impact of data protection on the adoption of digital technologies. The framework further focuses on determining

the concept of data protection and security by aligning with significant challenges that occur due to phishing attacks, malware, and ransomware. The conceptual framework explains that the independent variable which is data transformation results in affecting the dependent variable which is data protection because of factors including phishing attacks, malware, and ransomware within the Omani SMBs. Extensive exploration on the research objectives by aligning with the theoretical framework, the study helps understand the impact of data protection issues on data transformation within SMBs in the Omani context. Further, the conceptual framework also helps in determining the data-related issues mainly faced by the management as a result of technical progress and inadequate security.

2.7. Hypothesis Statements

Based on the conceptual framework and literature review, current literature gaps have been identified. Following this, the null and alternative hypotheses have been formulated by aligning with the research questions:

Hypothesis one

Null Hypothesis ($H_0$1): There is no impact of digital transformation on the data-related issues in SMBs.

Alternative Hypothesis (H_a1): There is a significant impact on the data-related issues in SMBs.

Hypothesis two

Null Hypothesis ($H_0$2): No data-related difficulties have been identified within SMBs management as a result of inadequate security and technical progress.

Alternative Hypothesis (H_a2): Significant data-related difficulties have been identified within SMBs management as a result of inadequate security and technical progress.

Hypothesis three

Null Hypothesis ($H_0$3): No recommendations have been determined in reducing cybersecurity threats in SMBs.

Alternative Hypothesis (H_a3): Significant recommendations have been determined in reducing cybersecurity threats in SMBs.

2.8. Summary of the Literature Review Chapter

This chapter offered a comprehensive review of academic literature that are relevant in investigating the main research problem regarding the impact of data-related issues on digital transformation, data-related challenges faced by organizational management as a result of technical progress and inadequate security, and the recommendations that are helpful in addressing the challenges and preventing the risks related to data. The research has been conducted to understand the conceptual foundations comprehensively while providing enhanced knowledge about the adoption of digital transformation within SMBs along with its efficacy after its implementation. As the pandemic has led to the shift towards digital transformation, it offers SMBs with multifaceted benefits to businesses. Despite these benefits, the adoption of these digital transformations has also led to several challenges that resulted in affecting the business operations and consumer base at the same time. In addition to this, the research also conducted on the challenges faced by the management especially on technical progress and inadequate security of the advanced digital technologies. Further, the research also emphasized on discussing the recommendations that fight against these data-related issues and cybersecurity threats within SMBs. Thus, the chapter gives a detailed understanding of the impact, challenges faced, and recommendations based on the adoption of digital transformation and data protection within Omani SMBs.

The chapter further discusses some of the important theoretical frameworks including the TAM model framework, risk assessment framework, and the GDPR framework. The TAM framework provides a deep understanding of the adoption of

digital technologies within businesses by further making it clear to understand the impact and usage effectively. Further, the risk assessment framework also focuses on the risk management approach that can be considered by organisations to manage the determined challenges. Additionally, the GDPR framework focuses mainly on the protection and security of data ensuring to prevent data from cyber threats.

The chapter further continues with a thorough introduction to the digital transformation and its adoption within SMBs. The research also highlights the capabilities, benefits, and constraints of shifting towards digital transformation, especially within small and medium-sized businesses. The benefits offered by the implementation of this technology especially during the pandemic resulted in operating the business. This led to the increased adoption of digital technologies. However, adopting these technologies not only offered benefits but it also affected customers negatively by eroding away their trust on the protection of sensitive information.

Further, the chapter emphasizes on determining the key challenges faced by the management that result in inadequate security of data and technical progress. The research further focused upon explaining the concept of data protection within organisation, and then identify the challenges faced by SMBs to manage and protect data in Oman. The research then emphasizes on discussing the gaps in data security and technical progress. As the challenges and gaps have been identified, now the study emphasized on determining significant recommendations to determine the strategies that help recover from digital disaster and also help boost the economy while ensuring that the business also earns profits. Additionally, the research also emphasizes on discussing the strategic planning for cyber threats.

The next section involves discussing the knowledge gaps determined from the literature review revealing a lack of studies focusing on the technical progress, and offering adequate information on data protection and security. Further, fewer studies have also determined with a focus on recommending strategies to fight against cyber threats. The chapter then continues its discussion with the conceptual framework by determining

the independent and dependent variables by aligning with the research objectives and theoretical framework. Lastly, the chapter states the hypothesis based on the research questions and conceptual framework.

Thus, the next chapter of the research methodology will employ appropriate methods to test and explore the impact of data-related issues on the adoption of digital transformation within SMBs, especially in the Sultanate of Oman.

CHAPTER III:

METHODOLOGY

3.1 Brief Introduction to the Chapter

Research methods in a study serves as an important method with the help of which the research plans, designs and gathers relevant data from the reliable sources in order to answer the research questions. This often refers to as the strategies that allow the researcher to conduct the study in a structured approach. Further the structured approach empowers the researcher to investigate the research problem in an ethical manner and hence contributes to the conclusion of the study. Thus, this chapter of the study outlines the methods, techniques, and processes that the researcher has employed in order to conduct the study.

Thus, the chapter begins by explaining with the research problem and what has influenced the researcher to conduct the study in this context. And the understanding of the research problem has allowed the researcher to construct the research questions. The researcher has described the research methods, which serves as the blueprint for conducting the study. Thus, this section reveals whether the research follows a qualitative, quantitative, or mixed-method approach, depending on the nature of the problem and the objectives of the study. Followed by this the researcher defines the research design, research approach and research philosophy. Moreover, this chapter of the study has also shed light into the data collection techniques that the researcher has adopted to gather relevant data. And based on the collected data the researcher has discussed the data analysis method which has allowed the researcher to interpret the data has further has allowed to contribute to the findings of the study. In addition to this the researcher has also defined the ethical considerations, including informed consent, data privacy, and research integrity, are also addressed to ensure compliance with ethical research standards. And the last section of the chapter defines the research limitations.

3.2 Overview of the research problem

This study includes data from OECD nations. The greatest attempts have been taken to mention sources that use representative samples, have precise and well-defined questions, and break down the results by enterprise size. Data on digital events and data breaches that are comparable across borders is still lacking, though. To assist in gathering more comparable and higher-quality data locally, between 2016 and 2018, a survey questionnaire and measurement methodology were developed by the OECD Working Parties on Measuring and Examination of the Digital Economy (MADE) and Security and Privacy in the Digital Economy (SPDE).

Few OECD nations have used this technique up to this point. This limits the range of nations covered in this study. There are a number of methodological problems with data on digital security events, such as non-representative and non-random sampling, underreporting due to legal or reputational concerns, or disparities in detection and measurement capabilities between businesses.

Furthermore, coverage by business size varies significantly between sources. The surveys used in this article were chosen because they do not have the non-representative and typically non-randomised sample problems that are prevalent in the literature and research on digital security and data protection. However, across OECD nations, businesses of the same size or in the same industry tend to exhibit the same tendencies as those outlined in this document.

The extent to which the OECD standard assessment framework has been adopted across members is low because the process of standardizing digital security is not without systemic issues. However, they include issues like the availability of resources, variations in policies governing the countries involved, and other competing agendas that do not have much support for implementation. For instance, some economies may simply be unable to conduct detailed studies and measures and still others may focus on establishing local cybersecurity measures rather than international synchronization. Thus, it deepens the problem of siloed data environments, making it difficult to compare the successes and failures across countries or to determine the overall state of the world. In

addition, incidents may be underreported, and an organization might not report them if they think they may attract regulatory action or if markets do not have confidence in the organization. Such gaps are unhelpful in the policy formation process especially where governments and businesses use limited information to create strategies on resource allocation or defence. Also, as much as the selected surveys reduce sampling bias, the nature of cyber threats, including the types of attacks and strategies and the imbalance in the ability to detect threats, are not considered. Two aspects of the future activity could be developed further: the incorporation of real-time data-sharing systems to reduce data duplication, and the promotion of closer collaboration between nonprofit and for-profit organizations to improve the degree of openness. This is important to solve such issues to create sustainable approaches that encapsulate the changing nature of threats and opportunities in different economic systems.

3.3 Research Philosophy

Research philosophy refers to the set of beliefs and assumptions that guide the researcher in conducting the study. This is the process where the researchers view the nature of reality (ontology), the process of gaining knowledge (epistemology), and the role of values in research (axiology). Thus the research philosophy can be defined as the naturalistic, and shared belief that allows to analyze and understand different concepts relevant to the topic. This allows the researcher to analyze a particular context on the basis of their point of view, assumptions and shared ideas. Thus, with an in-depth understanding of the research philosophy, this allows in selecting the appropriate research methods and strategies.

A research philosophy is of three types that are namely positivism, interpretivism and pragmatism. A positivism research philosophy primarily relies on data and statistical analysis. Further the interpretivism research philosophy mainly focuses on subjective experiences emphasising on the traditional and cultural contexts which often can be understood from the case studies. And lastly a pragmatism research philosophy is a belief

that the findings of the study should be driven from the practical outcomes rather than considering the outcomes of the specific philosophy. But the selection of the research philosophy depends on the aims and objective of the study and the chosen research methodology of the research.

Therefore, the choice of the research philosophy in this study is closely connected with difficulties in the process of international data comparability and the practical requirement to provide useful recommendations in the sphere of digital security. Due to methodological differences and the break-up in reporting in OECD datasets, the study is most appropriately situated in a pragmatic paradigm because it is more concerned with the practical use of knowledge than with epistemological purity. This approach allows for quantitative data, such as the survey results of breaches, to be merged with qualitative information on contextual influences such as the regulations or culture towards cybersecurity. In using pragmatism, the research holds the view that the purely positivist methodologies, such as over-dependence on part statistics, are out of merit, but at the same time, this research does not cuddle to extreme interpretivism that hails overly subjective and personal narratives at the detriment of normative trends. Based on this conceptualization, the ontology employed here is intersubjective, where digital security risk is realized through counts and rates of incidents and structures such as reporting culture. Methodologically, the work is qualitative and quantitative at the same time as it is assumed that detection capacities and reporting tendencies are different within enterprises and countries. Methodologically, the research respects the principles of axiological transparency and cross-country comparability which is in line with the OECD's mission in coordinating policies at the international level. This philosophy therefore informs the choice of methods like combined surveys and case studies to bridge the gap in the detection and representation while arriving at the conclusion that can have a worldwide applicability.

3.3.1 Selection of research philosophy and justification

As the researcher has chosen quantitative research methodology for conducting this study, thus depending on the nature of the chosen research methodology, the researcher has chosen positivism research philosophy. Given that the study seeks to conduct a gap analysis and assess risk mitigation strategies, the chosen philosophy has enabled for a structured and systematic investigation of the chosen context. Also the chosen philosophy has allowed the researcher to rely on empirical data collection, ensuring that findings are based on observable and reliable evidence rather than subjective interpretation. It is believed that the positivism research philosophy was relevant while examining the impact of digital transformation on the data protection issues and the associated risk mitigation strategies in order to solve the cyber security threats experienced by the SMBs on Oman in the post pandemic situation. The data driven recommendations for SMBs will further empower the them to improve cyber security frameworks and regulatory compliance, ensuring that risk mitigation strategies are built on factual evidence rather than anecdotal perspectives. Additionally, positivism enhances the reliability and validity of the findings of the study, allowing for generalizable conclusions that can be applied across similar business contexts.

The choice of positivism corresponds to the quantitative approach and the study's focus on cross-country comparisons as well as the OECD's requirement for methodological and empirical analysis of policy issues. Positivism therefore reduces bias originating from disparate sets of incidents since they can sometimes vary with culture or institution in other regions. That is exactly the philosophy that would enable one to quantify relations between digital transformation and cybersecurity threats, like the relation between enterprises' size and breach rates, which is important to compare SMBs in Oman with OECD countries. Moreover, as positivism does not allow for interpretative subjectivism, the study's call for regulatory reforms is more persuasive to policymakers since they depend on numbers to justify funding for cybersecurity development. It also responds to Oman's post-pandemic digital intensification, meaning that relative proportionality rates on threat factors as working from home risk relevance- are obtainable to carry out preventive actions. Through statistical analysis, the findings

establish connections between regional issues and global solutions, which provides a strong foundation for SMBs as they combat continuously emerging cyber threats.

3.4 Research Design

A research design is a systematic approach that enables the research to identify and interpret the observations and thus allows in answering the designed. Thus, a research design also helps the researcher with the structure and data collection strategy. A research design is of two type's explanatory and exploratory categories.

An explanatory research design aims to develop a cause-and-effect relationship between the variables and thus allowing the researcher to explain why and how the certain phenomenon has occurred. And this can be done through statistical data analysis method. On the other hand, exploratory research design is used to investigate an unknown problem, and which needs to be investigated to have a clear picture of the problem.

The research method applied in the study involves an explanatory research design to analyze the causal factors of digital transformation and cybersecurity risks of Omani SMBs with the help of OECD data sets. This approach aligns with positivism which underlines hypothesis testing by statistical methods since the identification of patterns like how accelerated activities like cloud adoption are related to breaches after the pandemic is critical. Due to considering discrete variables (e.g. enterprise size, sector-specific risks), the design minimizes bias that stems from a lack of integral OECD data and allows for a structured horizontally comparative approach. This structure helps achieve the study's objective of applying the findings that can be used for designing containment strategies in Oman regarding the existing legal deficits and enriching the development of international standards. The structure properly incorporates elements that lead to recommendations that are crucial for policymakers in contexts characterized by asymmetrical threat dynamics thrown up by the changing nature of economies in the digital age.

3.4.1 Selection of research design and justification

Depending on the chosen research methodology, the researcher has chosen explanatory research design, it has enabled for a comprehensive understanding of the impact of digital transformation on the data protection issues faced by SMBs in Oman. Also, as this research design is appropriate for identify patterns, relationships, and underlying factors influencing a phenomenon thus this research design is an appropriate choice for the study. As in this study the researcher aims to understand the impact of digital transformation on data-related issues, and also assess the data management challenges that are faced by the SMBs in Oman and propose mitigation strategies utilizing an explanatory approach, has allowed analyzing the interdependencies between technological adoption and cyber security risks through empirical data collection and statistical analysis. Thus, this allows the researcher to provide actionable insights which can further empowers SMBs in Oman as well as policymakers in strengthening cyber security practices in Oman's evolving digital landscape, thus contributing to the economic development of the country.

The priority of the explanatory design lies in the possibility of revealing how Oman's post-pandemic fast-growing process, including cloud migration, remote work, etc., aggravates vulnerabilities in low cybersecurity readiness SMBs. Since OECD metrics are applied to this analysis, the study identifies variables (e.g., sector-based threat exposure or resource differences) that contribute to organizations' breach readiness beyond mere descriptive trend analysis. This also defines policies to address Oman's regulatory fragmentation that involve recommending changes in practices that conform with the OECD policy or framework (for instance, standardization of incident reporting). By stressing an empirical approach, the designed mitigation strategies address both technical threats, such as archaic encryption, and behavioral contributors to cyber risk and provide for interventions adaptable to Oman's socio-economic environment that may also potentially contribute to the development of transnational cybersecurity knowledge.

3.5 Research Methods

Research methods can be defined as the blueprint of the study that helps the researcher to conduct the study in a structured approach. A well-defined research methodology equips the researcher with all the strategies that are important in order to collect the data. This can be also defined as the roadmap, enabling researchers to conduct their study in an organized and logical manner. Thus, a well-structured research method enhances the validity, reliability, and accuracy of the findings. A research method is of three types that are namely quantitative, qualitative, and mixed research methods. Qualitative research primarily focuses on exploring concepts, behaviors, and experiences through interviews, observations, or case studies. On the other hand, a quantitative research methodology relies on numerical data, statistical tools, and measurable variables, often employs surveys, experiments, or secondary datasets to collect data. And lastly a mixed research methodology integrates both qualitative and quantitative approaches to provide a more comprehensive analysis. Thuson the basis of the research methodology the researcher gets an insight into the data collection technique.

3.5.1 Selection of research method and justification

A research method is chosen based on the research objectives or research questions that the researcher aims to address. Depending on the nature of the objectives of the study the stud has selected quantitative research methodology. The chosen methodology has enabled for the collection of numerical data, enabling statistical analysis to identify patterns, correlations, and trends in SMBs' digital security practices. With the help of the quantitative data, this has allowed to investigate the chosen context with the help of survey questionnaire where the researcher was allowed to gather real world data, thus making valuable contributions to the findings of the study. Also the methodology also enables the researcher for gathering large-scale data collection through structured surveys or questionnaires. And this further enhances the reliability of the findings of the study. With the help of the quantitative methods the research has evaluate the extent of cyber security vulnerabilities, compliance gaps, and has examined the effective risk mitigation strategies that can be applied among the SMBs in Oman. Also, as this ensures to offer reliability and generalizability of findings, this makes the findings of the study

applicable to a broader population or similar business culture in other countries as well. In addition to this the structural nature of this approach minimizes biasness and ensures to offer reliable conclusion. Thus, this can be said that the chosen methodology has strengthened the study's credibility and provided empirical evidence for recommending best practices for SMBs in Oman.

The quantitative method can provide data that matches with OECD's established measures, which is crucial in comprehending the position of Oman's SMBs against the background of global cybersecurity threats. Probability sampling allows counts of incidents, adherence, and resources, which are critical for comparing with well-developed nations in the OECD, towards which Nigeria aspires to be aligned in terms of data readiness. This also targets Oman's post-contamination digital terms by measuring new risks (such as increased phishing caused by telecommuting) and reviewing risk reduction measures (such as encryption scores). The approach helps eliminate response biases prevalent in cybersecurity research owing to the participants' hesitation and reluctance to reveal sensitive data through actual findings. Besides, the statistical approach can be used in the logical policy design, which allows Oman to meet the OECD standards and, at the same time, adapt solutions to the local issues of the infrastructural and cultural context, promoting the development of reliable, universality-based cybersecurity practices.

3.6 Research approach

A research approach refers to the set of plans and procedures which enables the researcher to make assumptions in order to gather information from the relevant sources. a research approach can be divided into two categories deductive and inductive.

A deductive research approach primarily initiates by considering a specific theory or hypothesis and further with the help of gathered information's or observations test the validity of the theory, through hypothesis testing. Thus, this approach guides the researcher in data collection and data analysis method. On the other hand, inductive approach begins with specific observations and patterns, leading to the development of broader theories or conclusions. Thus, a deductive approach often follows top-down

approach and on the other hand inductive approach follows a bottom-up process, allowing researchers to build new theories based on emerging data. The selection of the research approach is guided by research design.

3.6.1 Selection of research approach and justification

Thus, depending on the nature of chosen research design and methodology, the researcher has employed deductive research approach, and this has allowed the researcher to test the existing theories and frameworks in the context of data protection within SMBs of Oman. Also, the deductive approach is suitable for conducting a gap analysis, as it enables the comparison between theoretical cyber security standards and real-world practices observed in SMBs. Also, the deductive research approach allows in testing the defined research hypothesis and this allowed in developing a linkage between the independent variable and dependent variable. And the hypothesis testing allows to offer insight into whether the transformation to digital transparency has impacted the data security of the SMBs in Oman. This further helped in contributing to the conclusion of the study and has resulted in enhancing the results of the study.

The deductive approach enhances the rigor of the study to compare and contrast the OECD cybersecurity frameworks with the localized picture that SMBs face in Oman. Using the results of surveys with the application of the NIST Cybersecurity Framework or ISO 27001 policies, the approach highlights specific areas where policies are not implemented consistently (e.g., differences in reporting incidents) and measures the relationship between these gaps and breach rates. This same method is useful for positioning Oman's post-COVID-19 digital growth, meaning hypotheses that specify a bump in tech usage (JV) and an increase in vulnerability threats (DV it out. The top-down structure of the approach guarantees that its findings are meaningful to global policy players; simultaneously, it assumes a completely different position regarding Oman's specific infrastructural condition when it comes to IT investment – either its budget is insufficient, or its employees' skill gaps are too vast. This connects the abstract academic

contribution with concrete recommendations for SMB management with situational scenarios.

3.7 Hypothesis Development

To conduct the study on the chosen topic “Small and Medium-Sized Businesses (SMB) In Oman Data Protection in Digital Transformation Post-Covid 19 - Gap Analysis and Risk Mitigation”, the study has designed three hypotheses in order to the answer the research questions. The existing literature reviews in the similar context has enabled the researcher to form the hypothesis by considering independent and dependent variable.

3.7.1 Independent and Dependent variable

Conducting comprehensive literature reviews has allowed the researcher to understand that the outbreak of the COVID-19 has not only altered the way of living and communication but it has transformed how business used to perform and operate their organisational functions. And as a result of this, organisations irrespective of their sizes had to rely on digital platforms which empowered them to continue their organisational functions. The easy accessibility of the digital system has influenced to stay connected with the digital platforms and technologies and thus continue their operations in the post pandemic situation. Even though it has empowered the companies, but the negative side of the technologies posed challenges for them in terms of data security. In addition to this the SMBs of Oman are facing more challenges as compared to the large size business due to financial constraints. Thus, the researcher has conducted intensive literature reviews to understand this context and seeks to gain an insight on the impact of the of digital transformation in the post COVID-19 period on the data protection in the SMBs of Oman. And this has resulted in the development of the independent and dependent variable where the independent variable is digital transformation and on the other hand dependent variable is data protection. Thus, the hypothesis testing has allowed to offer an insight into the impact of digital transformation on the data protection in the SMBs of Oman.

3.8 Data collection Procedure

Data collection is the most important phase in the research process. Data collection procedure refers to the method where the researcher gathers data from the relevant resources. In other words, this can be also defined as systematic techniques used to gather information for research, decision-making, or analysis. This is an important aspect of any research, and this method enhances the findings of the study and contributes to analyzing specific assumptions or theories with the help of data. A data in research can be gathered form of observation, information and numerical data which further the researcher analyses with the help of appropriate data analysis method. Data are of two types one is primary data, and the other is secondary data, the primary data refers to the firsthand data where the collection procedure involves gathering firsthand information directly from sources. And on the other hand, secondary data refers to the information and are mainly relies on existing data sources. Thus, the primary data is gathered through survey or interview method and to some extent this can be collected from observation and experiments. Whereas secondary data are collected from publicly available resources, such as goggle scholar, government reports and databases and company records. Depending on the nature of the study and chosen research methodology the research has gathered primary as well as secondary data.

Apart from this the data collection procedure has considered inclusion and exclusion criteria. The inclusion criteria of the study were that the study has involved professionals from the SMBs of Oman. And on the other hand, exclusion criteria of the study were that this has not involved any participants below one years of experience.

3.8.1 Research Instrument and Development and Measurable Scales

The researcher in this study has employed closed ended survey questionnaire as a research instrument. A research instrument refers to a piece of document that empowers the researcher to gather primary or first-hand data from the selected participants. A research instrument can be in the form of survey questionnaire or interview, but the selection of the instrument depends on the nature of the chosen research methodology of

the current study. Thus, the survey questionnaire has allowed to collect primary data and on the other hand the researcher has gathered secondary data from the google scholar, ProQuest, research gate, etc.

The survey questionnaire was developed on the basis five-point Likert scale and the survey questionnaire was circulated to the SMBs of Oman to ensure anonymity of the participants and further the data was gathered through google forms. The first section of the questionnaire consisted of questions related to demographics and was measured using the nominal scale of measurement. The following highlights the four questions of the first section:

Q1. What is your age-group?

Q2. What is your role in the company?

Q3. In which industry are you working in?

Q4. How long have been operating your small and medium-sized business (SMB) in Oman?

The second part of questionnaire highlights questions to gain a deeper insight into the impact of digital transformation on data-related problems within SMBs. The following highlights the ten questions for hypothesis 1:

Q5. Do you agree that digital transformation has improved data management practices within your organisation?

Q6. Do you agree that the organisation has been impacted with the implementation of digital transformation in protecting sensitive information?

Q7. Do you agree with the fact that digital transformation leads to increased data-related issues within your organisation?

Q8. Do you agree that your organisation has experienced cyberattacks or data breaches since it has adopted digital transformation?

Q9. Do you agree that adopting digital transformation makes it easier for the organisation to protect sensitive information, and data?

Q10. Do you agree that the adoption of digital transformation within your organisation affects customer experience?

Q11. Do you agree that the implementation of digital transformation within your organisation impacts corporate efficiency?

Q12. Do you agree that digital transformation ensures regulatory compliance while improving document traceability?

Q13. Do you agree that digital transformation affects organisation by enhancing its operations intelligence?

Q14. Do you agree that digital transformation affects organisation by boosting its employee productivity?

The third part of questionnaire highlights questions to gain a deeper insight into the different problems faced by organization's management team. The following highlights the ten questions for hypothesis 2:

Q15. Do you agree that insufficient data storage is a major concern for your organisation?

Q16. Do you agree that inadequate data security measure is a problem for your organisation?

Q17. Do you agree that your organisation uses encryption to protect sensitive information, and data?

Q18Do you agree that your organisation works effectively on a clear data management strategy?

Q19. Do you agree that your organisation backs up sensitive data to prevent data loss and threats?

Q20. Do you agree that your organisation faces complexity in ensuring data compliance with regulatory requirements?

Q21. Do you agree that lack of data integration, and data silos acts as a hindrance for the organisation to make informed decisions?

Q22. Do you agree that the organisation lacks resources & expertise in order to manage data security?

Q23. Do you agree with the fact that the organisation lacks technical knowledge, and expertise to manage large datasets?

Q24. Do you agree that the organization's data analytics capabilities are limited because of inadequate technical resources?

The fourth part of questionnaire highlights questions to gain a deeper insight into the recommendations for minimizing cyber-security problems within SMBs. The following highlights the ten questions for objectives 3:

Q25. Do you agree with the fact that the implementation of robust cybersecurity measures can be considered for combating cybersecurity issues within SMBs?

Q26. Do you agree that regular cybersecurity audits are important for identifying, and reducing cybersecurity risks in SMBs?

Q27. Do you agree that SMBs need to invest in training for cybersecurity awareness?

Q28. Do you agree that SMBs should invest in cybersecurity threat measures?

Q29.Do you agree that SMBs should invest in cybersecurity insurance to prevent financial losses due to cyberattacks?

Q30.Do you agree that SMBs should limit and control account access in order to prevent cyberattacks?

Q31.Do you think it is important to enforce signed software execution policies for the eradication of cybersecurity measures?

Q32.Do you think it is important to have a close overview on the attack surfaces to mitigate cyberattacks?

Q33.Do you think it is important for your organisation to provide firewall security for the internet connection by not providing access to data on a private network?

Q34.Do you think it is significant for your organisation reset passwords and implement multi-factor authentication to gain access to the organisation`s network?

3.8.2 Validity Test

The validity test of a questionnaire is an important aspect of a research, with the help of this method, the researcher ensures that the selected research instrument accurately measures what it supposed to measure, and thus performing this test ensure the research findings are accurate and reliable. And also, the test enables the researcher to identify the errors in the selected research instrument, thus resulting in enhancing credibility of the research instrument and makes the findings of the study generalize so that it can be further applied in similar context.

In this research the researcher has employed content validity to test the accuracy of the research instrument.

3.8.2.1 Content Validity

The content validity enables the researcher to measure to what extent the developed research instrument has the potential to capture all the relevant aspects of the focused context. Thus, through this the researcher has examined the internal consistency of the research questionnaire. Further the questionnaire was validated by engaging 3 SMB owners and managers in Oman and also the method has also engaged 27 workers, who were IT personnel, employees and industry experts within SMBs who has an in-depth knowledge of the impact of digital transformation. These helped to identify the

actual issues in digital transformation. The individuals were distributed with the questionnaire and was also given with the purpose of the study.

3.8.3 Reliability Test

The reliability test in research is another important concept where the process allows to test the accuracy of the elements of the questionnaire. Thus, to ensure the reliability and validity of the questionnaire the researcher has conducted pilot test by involved 30 professionals from the SMBs within Oman. The participants were given with the survey questionnaire through google forms and further the researcher extracted the gathered transcript into excel. To perform the statistical data analysis, the researcher has converted the transcript into numerical data and followed by this step all the numerical data was imported into SPSS.

To analyses the reliability of the questionnaire of the researcher the researcher has performed reliability test through SPSS. And the reliability was examined with the help of the Cronbach alpha value. Where a Cronbach value above 0.70 is considered to reliable. Thus, this can has allowed to ensure the reliability of the research instrument. And thus, on ensuring the reliability and validity of the research instrument it was circulated to the broader population.

3.9 Research Population

Research population refers to the primary sources of information; this mainly involves people or individual who have knowledge on the chosen context. But selecting the research population needs to be match with some specific characteristics that the researcher sets depending on the nature of the study. The researcher involved those participants in the study whose age is above 18 years, and on the basis of their role, industry and experience in the SMB of Oman. In addition to this the targeted population was not restricted due to their gender and thus the research has involved both male and female in the data collection procedure. And also, no participants were allowed less than one-year experience in the chosen field. The research has chosen only professionals from the SMBs of Oman and their experience has helped to provide a deeper insight into the

challenges faced by SMEs in Oman in terms of data protection and cybersecurity. Further, the findings from the survey were used to identify potential solutions and recommendations for SMEs to improve their data protection practices and enhance their overall cybersecurity system. Additionally, the results from this research can be used as a reference for policymakers and stakeholders to better understand the needs and challenges faced by SMEs in Oman and provide support to help them overcome these challenges.

3.10 Sample Size Determination

Sample size refers to the number of the participants that the researcher includes in the data collection procedure. Thus, in this the research has determined the sample size of the study with the help of the Finite Populations Correction Factor:

For finite population correction factor:

$$n' = \frac{n}{1 + \frac{n}{N}}$$

Where: n = sample size for unlimited population; = finite population correction factor; N = Population size (taken in consideration = 141,126) (Times of Oman, 2024)

Z= Z-value of Confidence interval (taken at 95%=1.96); p= proportion of the sample population (taken as 0.15); e= margin of error (5% or 0.05)

$$n = \frac{Z^2 \times p \times (1 - p)}{e^2}$$

$$\frac{1.96^2 \times 0.15 \times (1 - 0.15)}{0.05^2}$$

This gives us a sample size of 195.90, rounded to 196 for infinite population(n=196).

For finite population correction factor: with N = Population size (taken in consideration = 141126)

$$n' = \frac{n}{1 + \frac{n}{N}}$$

$$= \frac{196}{1 + (\frac{196}{141126})}$$

This gives us a sample size of 195.80, rounded to 196. However, the research has involved 200 participants in the data collection procedure.

3.11 Sampling Technique

Sampling technique refers to the method used to select individuals or groups from a population to participate in a study. It ensures that the collected data represents the larger population without involving the large population in the survey method. There are two types of sampling technique that are probability sampling and non-probability sampling. Here the researcher has chosen non-probability sampling which has four types. As the study has selected participants based on specific characteristics the researcher has chosen purposive sampling technique. This has empowered the researcher in selecting appropriate participants in the survey (Adebayo and Ackers, 2021).

For conducting the pilot study, the researcher has selected 30 top management team of the SMBs who has in-depth knowledge of the challenges and digital tool. And further the researcher has involved 250 participants for the data collection procedure. The chosen sampling technique has further allowed to involve appropriate participants in the data collection procedure process. Also engaging individuals with relevant expertise ensures that responses are meaningful and informed rather than random. Also, the sampling technique has also allowed for gathering accurate, detailed, and practical insights. Thus with the help of this sampling technique the researcher has ensured that the

findings are valid, reliable and actionable, thus helping them identifying effective strategies that may help in mitigating the issues related to the data protection.

3.11.1. Pilot Study Results

Table 3.1: Pilot study for overall data

Reliability Statistics

Cronbach's Alpha	N of Items
.795	30

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Q5	113.40	88.800	.447	.783
Q6	113.50	90.741	.475	.785
Q7	113.67	92.575	.185	.794
Q8	113.70	94.148	.049	.802
Q9	113.50	91.569	.321	.789
Q10	113.50	89.362	.459	.783
Q11	113.77	89.771	.434	.784
Q12	113.53	89.016	.538	.781
Q13	113.47	88.189	.580	.779
Q14	113.63	86.516	.541	.778
Q15	113.50	86.741	.546	.778
Q16	113.60	89.007	.357	.786
Q17	113.90	91.817	.231	.792
Q18	114.03	88.654	.435	.783
Q19	113.63	87.137	.529	.779
Q20	114.97	94.723	-.003	.809
Q21	113.80	90.166	.423	.785
Q22	115.10	94.507	.000	.810
Q23	114.97	98.378	-.150	.820
Q24	115.00	100.207	-.216	.824
Q25	113.33	92.851	.323	.790
Q26	113.53	92.120	.414	.788

Q27	113.57	90.668	.460	.785
Q28	113.67	88.023	.550	.780
Q29	113.60	87.903	.529	.780
Q30	113.70	88.562	.459	.783
Q31	113.53	88.602	.490	.782
Q32	113.67	86.299	.681	.775
Q33	113.63	88.585	.434	.783
Q34	113.87	90.326	.281	.790

Table 3.2: Pilot study for objective 1

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.807	.818	10

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Q5	37.33	17.264	.565	.577	.781
Q6	37.43	19.151	.443	.466	.796
Q7	37.60	17.697	.473	.630	.792
Q8	37.63	17.620	.345	.610	.805
Q9	37.43	17.771	.602	.447	.779
Q10	37.43	18.185	.477	.443	.791
Q11	37.70	18.838	.373	.507	.802
Q12	37.47	18.464	.486	.366	.791
Q13	37.40	17.421	.655	.643	.773
Q14	37.57	16.944	.543	.649	.783

Table 3.3: Pilot study for Objective 2

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.601	.577	10

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Q15	30.60	22.731	.066	.538	.599
Q16	30.70	22.217	.103	.466	.592
Q17	31.00	24.828	-.183	.683	.557
Q18	31.13	23.223	.010	.764	.625
Q19	30.73	21.582	.218	.706	.588
2Q20	32.07	16.478	.587	.824	.480
Q21	30.90	20.783	.435	.295	.555
Q22	32.20	16.234	.581	.800	.479
Q23	32.07	16.754	.503	.796	.504
Q24	32.10	18.231	.349	.797	.556

Table 3.4: Pilot study for Objective 3

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.868	.866	10

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if

		Item Deleted			Item Deleted
Q25	36.83	22.420	.380	.636	.867
Q26	37.03	23.206	.219	.703	.863
Q27	37.07	20.823	.608	.702	.855
Q28	37.17	18.902	.779	.892	.839
Q29	37.10	18.576	.790	.900	.837
Q30	37.20	19.062	.672	.702	.848
Q31	37.03	19.206	.701	.677	.845
Q32	37.17	19.730	.637	.667	.851
Q33	37.13	19.085	.632	.813	.851
Q34	37.37	20.033	.423	.732	.874

3.12 Survey Questionnaire distribution and procedure

The distribution process of the research instrument is considered as another important aspect in a research. As the study has conducted survey, the researcher has circulated the questionnaire through mail, where the participants were asked to answer or share their opinion through google form on the basis of a five point Likert scale. The distribution strategy of the questionnaire was stick through one channel and this has allowed to maintain easy accessibility. And also this has enabled the researcher to maintain confidentiality of the respondents from the different SMBs in Oman who engaged themselves in the data collection procedure.

3.13 Statistical Test Used for analysis of the Data

3.13.1 Data encoding

As the researcher has gathered data through Google Forms where the participants had to share their opinion based on a closed ended questionnaire i.e for every question they were required to share their opinion based on a five-point scale (from 1 to 5), where 1= “Strongly Disagree”, 2= “"Disagree”, 3= "Neutral”, 4= "Agree”, 5= “Strongly agree".

Thus after the collecting the data the researcher the researcher encoded into the required form in order to perform the statistical analysis. And the data encoded from excel after extracting the transcripts from the google form. Followed by this step the data was analysed with the help of a statistical software known as SPSS and this has allowed in interpreting the primary data and thus contributed to findings of the study.

3.14 Data Analysis

Data analysis refers to the method where the researcher analyses the gathered data in order to address the developed research objectives. In this research as the research has gathered chosen quantitative research method, thus the researcher has analysed the primary data with the quantitative data analysis method. So, firstly the validity of the questionnaire was performed through content validity and the reliability of the questionnaire was analysed with the help of Cronbach's alpha. Further the researcher has performed correlation analysis to determine the impact of digital transformation on data-related problems within SMBs. Further the researcher has performed multiple regression in order examine the problems faced by the organisation and which further leads to inadequate security and technical progress.

3.15 Ethical Statement

Ethical considerationis paramount while conducting a research based on quantitative research methodology. The researcher significantly considers the research ethics to maintain all the fundamental principles of conducting the research and gathering data by properly following the guidelines and rules to collect true, relevant, and valuable information.

To conduct this study, the researcher has ensured to adhere all the ethical principles in order to enhance reliability of the findings of the study. Thus in this study the researcher has ensured to take informed consent form the participants, this has been followed to ensure that no participants were forced to participate in the data collection procedure. Before taking the consent from the participants the researcher offered an

understanding of the purpose of the study and also consent form outlined their right to withdraw at any stage without facing any consequences. This has ensured to maintain transparency between the researcher and the participants. And also to ensure there is no in transparency the participants were free to ask the researcher any questions in context to the research topic, data process, etc. Thus after clearing all the doubts, the participants were taken with consent and they were also informed that they are free to withdraw their participation at any moment of the survey without giving any reasons. Apart from this as the research has gathered primary data with the help of closed ended questionnaire, the researcher has ensured to maintain anonymity during the data collection procedure and thus no participants where asked with their name and also no participants were asked to share personal details. Further to ensure the confidentiality of the data, the researcher has saved the gathered information in a password protected device. The respondent was allowed to share their opinion through mail without feeling under any form of pressure, from the researcher. Apart from this the research has gathered secondary information from the reliable sources, this has ensured to put accurate information which are true and are applicable to real world scenarios. Thus all these considerations have allowed to enhance the credibility of the research findings.

CHAPTER IV:

RESULTS

4.1. Overview of the Chapter

This section of the research study provides a detailed knowledge of the findings that are determined by analyzing the quantitative data gathered by conducting survey. This offers a comprehensive and valuable insights to understand the research questions in a detailed manner. The chapter further focuses on the data gathering process where the data is gathered through primary method and the secondary information is gathered through existing scholarly sources. To conduct the survey, 200 participants from different roles and varying industries have participated from Oman. And the data was gathered within a time-period of 1 month while ensuring that all the involved participants had at least 1 year of experience. Further, all these data were considered for analysis and determine the findings based on the experience level, knowledge and understanding of the issues related to data when implementing digital technologies within the organisations.

To analyse the data, the research has utilised statistical methods and techniques, which is done with the help of a statistical software SPSS. It is considered as the most important tools to analyse quantitative data because it handles and interprets large sets of data easily. Moreover, as the study has used a 5-point Likert scale to collect the data, the software can analyse the data more easily. The raw data is initially imported into the SPSS software which is organized and transformed efficiently to produce valuable and meaningful numerical responses. Further, the analysis helps in the extraction of key findings from the gathered quantitative data.

The study also aligns the quantitative analysis with the proposed hypothesis to offer valuable insights and have an in-depth understanding of the research context. In addition to this, the research discusses the secondary findings from the scholarly sources explained in Chapter 2 to enrich the primary findings with a wider scope of secondary

landscape. This helps in developing a knowledge of practical implications. Before discussing the main findings of the study, the main objectives of the study are as follows:
RO1. Analyse how the digital transformation has affected the organisation's data-related problems in small and medium-sized businesses.
RO2. To assess various data-related difficulties that the management is facing as a result of inadequate security and technical progress
RO3. To make a better recommendation that assists in reducing the problems with cyber security in small to medium-sized businesses.

4.2. Demographic Analysis

This section presents some of the personal information of the participants without revealing their identity. These information include their age-group, role in organisation, industry in which the participant is working, and experience in specific field.

4.2.1. Age-group

Table 4.1. shows the age-group of participants involved in the survey. Out of 200 participants, 24% of them belonged from the youngest age group, that is, 18-25 years and the least number of participants who participated were aged above 60 years. Further, participants who were aged between 46-60 years were also in smaller proportion with 18.5%. Thus, the demographic findings on age-group suggested different perspectives of participants from varying age-group are encapsulated in the research. This further indicates that the participants belonging from different age-groups have substantial proportion of knowledge about the adoption of digital transformation and data-related issues in Omani SMBs.

Table 4.1: Age-group

What is your age-group?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-25 years	48	24.0	24.0	24.0
	26-35 years	41	20.5	20.5	44.5

	36-45 years	40	20.0	20.0	64.5
	46-60 years	37	18.5	18.5	83.0
	Above 60 years	34	17.0	17.0	100.0
	Total	200	100.0	100.0	

4.2.2. Role in Organisation

Table 4.2 indicates the role of participants in their organization. The statistical results indicated that 24% of the participants were data manager, however, 15% of participants involved in the survey were the founder of the organization. This suggested that the hands-on experience and strategic views of the participants belonging from different roles investigated the shift towards digital transformation and issues related to data, especially in SMBs in Oman.

Table 4.2: Role

What is your role in the company?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Founder	31	15.5	15.5	15.5
	IT manager	38	19.0	19.0	34.5
	Security manager	39	19.5	19.5	54.0
	Data manager	48	24.0	24.0	78.0
	Others (Please Specify)	44	22.0	22.0	100.0
	Total	200	100.0	100.0	

4.2.3. Type of industry

Table 4.3 indicates the type of industry in which the participant is working. A large proportion of participants with 27% were working in finance industry while only

14% of the participants were working in the manufacturing industry. Other participants belonged from different working sectors where 19% were from technology industry, 20% were from healthcare industry, and 19% were from retail industry. Thus, the demographic industry findings suggested perspectives of participants from different industries about the adoption of digital transformation and data-related issues in Omani SMBs.

Table 4.3: Type of Industry

In which industry are you working in?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Technology	38	19.0	19.0	19.0
	Healthcare	41	20.5	20.5	39.5
	Finance	55	27.5	27.5	67.0
	Retail	38	19.0	19.0	86.0
	Manufacturing	28	14.0	14.0	100.0
	Total	200	100.0	100.0	

4.2.4. Working Experience

Table 4.4 indicates the experience level of participants in their specific field. The results showed that a larger proportion of participants with 26% had an experience level more than 5 years and only 11.6% had an experience level of more than 1 year. Further, the results also shows that 16% participants had more than 15 years of experience, 22% participants had more than 2 years of experience, and 23% participants had more than 10 years of experience. Thus, this indicated that the participation of the participants offers credibility to the research and their understanding and knowledge about the digital transformation and data-related issues in SMBs facilitate and contextualize the data-related issues faced by SMBs in Oman.

Table 4.4: Working experience

How long have been operating your small and medium-sized business (SMB) in Oman?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	More than 1 year	23	11.5	11.5	11.5
	More than 2 years	45	22.5	22.5	34.0
	More than 5 years	52	26.0	26.0	60.0
	More than 10 years	47	23.5	23.5	83.5
	More than 15 years	33	16.5	16.5	100.0
	Total	200	100.0	100.0	

4.3. Reliability Test

Table 4.5. indicates the overall reliability of the data gathered by conducting survey. The overall reliability of the data is determined to be 0.921. This indicates that the determined value is valid and credible. This is so as the decision value of Cronbach-alpha is more than 0.6. If the value of Cronbach-alpha value is greater than 0.6, the data is considered to be credible. Thus, the result indicated that the credibility of the overall data is higher.

Table 4.5: Reliability Statistics of overall data

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on	N of Items

	Standardized Items	
.921	.933	30

Table 4.6 shows the value of Cronbach-alpha if item deleted, indicating that the value of all the questions except 5 questions are below 0.921. This indicates that if any of these questions are deleted, it would not improve the results of the Cronbach alpha for the entire data. However, as some of the Cronbach-alpha if item deleted values are higher than 0.921 which indicates that if these questions are deleted, it would result in improving the Cronbach-alpha value.

Table 4.6: Item-total statistics for overall data

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Q5	113.20	213.032	.783	.	.915
Q6	113.04	213.290	.784	.	.915
Q7	113.12	214.153	.747	.	.915
Q8	113.12	216.408	.652	.	.917
Q9	113.13	218.998	.633	.	.917
Q10	113.12	216.524	.664	.	.916
Q11	113.21	217.742	.662	.	.917
Q12	113.13	220.984	.577	.	.918
Q13	113.13	214.502	.740	.	.915
Q14	113.19	216.935	.656	.	.917

Q15	113.16	216.041	.727	.	.916
Q16	113.03	216.351	.712	.	.916
Q17	113.15	215.957	.699	.	.916
Q18	113.27	217.402	.611	.	.917
Q19	113.24	215.658	.723	.	.916
Q20	115.21	242.465	-.256	.	.931
Q21	114.04	224.039	.314	.	.922
Q22	115.22	242.019	-.239	.	.931
Q23	115.34	244.617	-.300	.	.932
Q24	115.32	246.066	-.336	.	.933
Q25	113.15	215.324	.767	.	.915
Q26	113.00	216.080	.764	.	.915
Q27	113.11	217.512	.712	.	.916
Q28	113.11	216.671	.695	.	.916
Q29	113.20	217.896	.648	.	.917
Q30	113.23	215.200	.708	.	.916
Q31	113.16	216.226	.691	.	.916
Q32	113.15	216.436	.703	.	.916
Q33	113.26	215.711	.642	.	.917
Q34	113.23	218.587	.546	.	.918

For objective 1

Table 4.7 indicates the reliability of the data gathered by conducting survey. The reliability of the questions under objective 1 is determined to be 0.934, indicating that the values are highly credible and valid. As the Cronbach-alpha value is greater than 0.6, it

can be considered as credible. Thus, the results indicated that the questions under objective 1 are valid and credible.

Table 4.7: Reliability statistics for objective 1

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.934	.934	10

Table 4.8 indicates the value of Cronbach-alpha if item deleted, indicating that the value of all the questions under objective 1 are below than 0.934. This indicates that if any of these questions are deleted from this objective, it would not result in improving the Cronbach-alpha value of objective 1.

Table 4.8: Item-total statistics for objective 1

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Q5	38.22	39.650	.787	.675	.925
Q6	38.06	39.785	.786	.666	.925
Q7	38.14	39.910	.770	.624	.926
Q8	38.14	40.145	.738	.571	.928
Q9	38.16	41.498	.710	.555	.929
Q10	38.14	40.412	.733	.573	.928
Q11	38.23	41.344	.698	.504	.930

Q12	38.15	42.379	.654	.485	.932
Q13	38.15	39.706	.798	.676	.925
Q14	38.21	40.740	.711	.574	.929

For objective 2

Table 4.9 indicates the reliability of the data gathered by conducting survey. The reliability of the questions under objective 2 is determined to be 0.596, indicating that the values are likely to be credible and valid. As the Cronbach-alpha value is below than 0.6, it can be considered more likely to be credible. Thus, the results indicated that the questions under objective 2 are likely to be valid and credible.

Table 4.9: Reliability statistics for objective 2

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.596	.602	10

Table 4.10 indicates the value of Cronbach-alpha if item deleted, indicating that the value of all the questions under objective 2 except 1 question are below than 0.596. This indicates that if any of these questions are deleted from this objective, it would not result in improving the Cronbach-alpha value of objective 2. However, 1 Cronbach-alpha if item deleted value is 0.600 which indicates that deleting this question would result in improving the value of Cronbach-alpha value for objective 2.

Table 4.10: Item-total statistics for objective 2

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Q15	28.58	19.079	.246	.557	.576
Q16	28.46	19.335	.209	.586	.583
Q17	28.58	19.823	.130	.596	.600
Q18	28.69	19.099	.207	.542	.584
Q19	28.66	18.829	.269	.553	.571
Q20	30.63	17.883	.293	.668	.564
Q21	29.47	16.290	.498	.280	.508
Q22	30.64	17.377	.342	.702	.551
Q23	30.77	17.628	.279	.667	.569
Q24	30.74	17.972	.235	.620	.581

For Objective 3

Table 4.11 indicates the reliability of the data gathered by conducting survey. The reliability of the questions under objective 3 is determined to be 0.930, indicating that the values are highly credible and valid. As the Cronbach-alpha value is greater than 0.6, it can be considered as credible. Thus, the results indicated that the questions under objective 3 are valid and credible.

Table 4.11: Reliability statistics for objective 3

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items

.930	.931	10

Table 4.12 indicates the value of Cronbach-alpha if item deleted, indicating that the value of all the questions under objective 3 are below than 0.930. This indicates that if any of these questions are deleted from this objective, it would not result in improving the Cronbach-alpha value of objective 3.

Table 4.12: Item-total statistics for objective 3

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Q25	37.95	39.626	.705	.635	.924
Q26	37.80	39.508	.748	.692	.922
Q27	37.91	39.906	.717	.585	.923
Q28	37.91	39.168	.734	.654	.922
Q29	38.00	39.231	.732	.636	.923
Q30	38.03	38.306	.767	.670	.921
Q31	37.96	38.561	.770	.693	.921
Q32	37.94	38.786	.772	.698	.921
Q33	38.06	37.996	.739	.658	.922
Q34	38.03	39.622	.601	.514	.930

4.4. Descriptive Statistics

For Objective 1

Table 4.13 shows the value of descriptive statistics which focus mainly on the mean, standard deviation, minimum and maximum range, and the values of skewness and

kurtosis. The table indicates that the mean value for the questions under objective 1 is close to 4 and the value of standard deviation mainly ranges between 0.8 and 0.9 indicating that the values are close to the mean value indicating that the data is highly dispersed. The maximum and minimum value ranges between 5 and 1. Further, the skewness value ranges between -1 and -2. As the value of skewness is negative, it indicates that the distribution of the questions are slightly skewed to the left. The kurtosis value ranges between 1 and 5 indicating that all the values are positive. This means that the distribution has heavier tails.

Table 4.13: Descriptive statistics for objective 1

Descriptive Statistics

	N	Range	Minimum	Maximum	Mean	Std. Deviation	Skewness		Kurtosis	
								Std. Error	Statistic	Std. Error
Q5	200	4	1	5	4.18	.928	-1.965	.172	4.703	.342
Q6	200	4	1	5	4.34	.916	-2.076	.172	5.046	.342
Q7	200	4	1	5	4.26	.920	-1.713	.172	3.386	.342
Q8	200	4	1	5	4.26	.930	-1.705	.172	3.252	.342
Q9	200	4	1	5	4.25	.824	-1.519	.172	3.273	.342
Q10	200	4	1	5	4.26	.909	-1.714	.172	3.522	.342
Q11	200	4	1	5	4.17	.851	-1.271	.172	2.179	.342
Q12	200	4	1	5	4.25	.788	-1.347	.172	2.799	.342

Q13	200	4	1	5	4.25	.912	-1.722	.172	3.517	.342
Q14	200	4	1	5	4.19	.899	-1.223	.172	1.539	.342
Valid N (listwise)	200									

For Objective 2

Table 4.14 shows the value of descriptive statistics which focus mainly on the mean, standard deviation, minimum and maximum range, and the values of skewness and kurtosis. The table indicates that the mean value for the questions under objective 2 is close to 2, 3, & 4 and the value of standard deviation mainly ranges between 0.5 and 1 indicating that the values are close to the mean value indicating that the data is highly dispersed. The maximum and minimum value ranges between 5 and 1. Further, the skewness value ranges between -1 and +1. As the value of skewness is negative, it indicates that the distribution of the questions are slightly skewed to the left. However, positive skewness value indicates that the distribution of the questions are not skewed to the left. The kurtosis value ranges between 1 and 5 indicating that all the values are positive. This means that the distribution has heavier tails.

Table 4.14: Descriptive statistics for objective 2

Descriptive Statistics

	N	Range	Minimum	Maximum	Mean	Std. Deviation	Skewness		Kurtosis	
								Std. Error		Std. Error
Q15	200	4	1	5	4.22	.857	-1.793	.172	4.513	.342
Q16	200	4	1	5	4.35	.860	-1.784	.172	3.879	.342
Q17	200	4	1	5	4.22	.894	-1.612	.172	3.195	.342
Q18	200	4	1	5	4.11	.934	-1.380	.172	2.242	.342
Q19	200	4	1	5	4.14	.880	-1.485	.172	3.169	.342
Q20	200	4	1	5	2.17	1.066	1.062	.172	.690	.342
Q21	200	4	1	5	3.34	1.058	-.473	.172	.086	.342
Q22	200	4	1	5	2.16	1.086	1.007	.172	.497	.342
Q23	200	4	1	5	2.04	1.153	1.102	.172	.431	.342
Q24	200	4	1	5	2.06	1.168	1.011	.172	.126	.342
Valid N (listwise)	200									

For Objective 3

Table 4.15 shows the value of descriptive statistics which focus mainly on the mean, standard deviation, minimum and maximum range, and the values of skewness and kurtosis. The table indicates that the mean value for the questions under objective 3 is close to 4 and the value of standard deviation mainly ranges between 0.8 and 1 indicating

that the values are close to the mean value indicating that the data is highly dispersed. The maximum and minimum value ranges between 5 and 1. Further, the skewness value ranges between -1 and +1. As the value of skewness is negative, it indicates that the distribution of the questions are slightly skewed to the left. The kurtosis value ranges between 1 and 5 indicating that all the values are positive. This means that the distribution has heavier tails.

Table 4.15: Descriptive statistics for objective 3

Descriptive Statistics

	N	Range	Minimum	Maximum	Mean	Std. Deviation	Skewness		Kurtosis	
							Statistic	Std. Error	Statistic	Std. Error
Q25	200	4	1	5	4.22	.847	-2.000	.172	5.643	.342
Q26	200	4	1	5	4.38	.817	-1.796	.172	4.185	.342
Q27	200	4	1	5	4.27	.806	-1.691	.172	4.437	.342
Q28	200	4	1	5	4.26	.865	-1.341	.172	1.878	.342
Q29	200	4	1	5	4.18	.861	-1.359	.172	2.572	.342
Q30	200	4	1	5	4.15	.917	-1.249	.172	1.686	.342
Q31	200	4	1	5	4.22	.890	-1.472	.172	2.780	.342
Q32	200	4	1	5	4.23	.867	-1.167	.172	1.341	.342
Q33	200	4	1	5	4.11	.978	-1.405	.172	2.167	.342
Q34	200	4	1	5	4.15	.965	-1.219	.172	1.213	.342

Valid N (listwise)	200									

4.5. Hypothesis Testing

4.5.1. Hypothesis One

$H_0$1: There is no impact of digital transformation on the data-related issues in SMBs.

H_a1: There is a significant impact on the data-related issues in SMBs.

Table 4.16 indicates the correlation between the variables under objective 1 that is, data transformation, and data-related issues. The results indicated the correlation value to be 0.862 which is very close to 1. As the correlation value ranges between -1 to +1, the decision value suggests that the value close to +1 indicates stronger positive value, and the value close to -1 indicates stronger negative value. The table shows Avg_Variable1 which indicates data transformation, and Avg_Variable2 which indicates data-related issues. The correlation indicates stronger positive relations between the adoption of digital transformation and data-related issues.

Table 4.16: Hypothesis one using correlation

Correlations

		Avg_Variable1	Avg_Variable2
Avg_Variable1	Pearson Correlation	1	.862**
	Sig. (2-tailed)		.000
	N	200	200
Avg_Variable2	Pearson Correlation	.862**	1
	Sig. (2-tailed)	.000	
	N	200	200

**. Correlation is significant at the 0.01 level (2-tailed).

Thus, the result indicates that the null hypothesis is rejected as there exists a significant relationship between the variables.

4.5.2. Hypothesis Two

$H_0$2: No data-related difficulties have been identified within SMBs management as a result of inadequate security and technical progress.

H_a2: Significant data-related difficulties have been identified within SMBs management as a result of inadequate security and technical progress.

Table 4.17 indicates the one-sample statistics for objective 2, explaining the mean, standard deviation, and standard error mean for the factors under objective 2. This explains that the mean values and standard deviation values are close to each other indicating that the data are highly spread out.

Table 4.17: Hypothesis two using one-sample statistics

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
Q15	200	4.22	.857	.061
Q16	200	4.35	.860	.061
Q17	200	4.23	.894	.063
Q18	200	4.11	.934	.066
Q19	200	4.14	.880	.062
Q20	200	2.17	1.066	.075
Q21	200	3.34	1.058	.075
Q22	200	2.16	1.086	.077
Q23	200	2.04	1.153	.082
Q24	200	2.06	1.168	.083

Following this, table 4.18 indicates the one-sample t-test for the same indicating that the p-value for all the factors under objective 2 has a significance value of 0.000 which is below than 0.05. This indicates a significant relationship between the factors technical progress, inadequate security, and data related challenges faced by organization. Further, the t-test value is also much higher than 1.96 explaining that the factors that management has a significant impact of data-related challenges because of technical progress and inadequate security.

Table 4.18: One-sample test

One-Sample Test

	Test Value = 3					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
Q15	20.121	199	.000	1.220	1.10	1.34
Q16	22.117	199	.000	1.345	1.23	1.46
Q17	19.389	199	.000	1.225	1.10	1.35
Q18	16.808	199	.000	1.110	.98	1.24
Q19	18.322	199	.000	1.140	1.02	1.26
Q20	-11.009	199	.000	-.830	-.98	-.68
Q21	4.480	199	.000	.335	.19	.48
Q22	-10.934	199	.000	-.840	-.99	-.69
Q23	-11.832	199	.000	-.965	-1.13	-.80
Q24	-11.386	199	.000	-.940	-1.10	-.78

Table 4.19 shows the One-way ANOVA table determining whether there is a statistically significant difference between the group means. The result suggested that the significance value is 0.001 which is below than the p-value (0.05). Thus, the result indicates statistically significant difference between the means of data-related challenges and technical progress and inadequate security.

Table 4.19: ANOVA

ANOVA

Avg_Variable3

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	1057.572	24	44.065	2.371	.001
Within Groups	3252.428	175	18.585		
Total	4310.000	199			

Thus, the result indicates that the null hypothesis is rejected as there is a significant impact between the variables.

4.5.3. Hypothesis Three

$H_0$3: No recommendations have been determined in reducing cybersecurity threats in SMBs.

H_a3: Significant recommendations have been determined in reducing cybersecurity threats in SMBs.

Table 4.20 indicates the correlation between Avg_var5 and Avg_var6, where Avg_var5 indicates the data transformation and Avg_var6 indicates the cybersecurity issues. As the correlation value ranges between -1 to +1, the result indicates robust positive relationship between the both the variables. The decision value suggests that if the value is close to +1, strong positive relationship exists, and if the value is close to -1, the relationship between the variables is strongly negative.

Table 4.20: Hypothesis three using correlation

Correlations

		Avg_var6	Avg_var5
Pearson Correlation	Avg_var6	1.000	.816
	Avg_var5	.816	1.000
Sig. (1-tailed)	Avg_var6	.	.000
	Avg_var5	.000	.
N	Avg_var6	200	200
	Avg_var5	200	200

Table 4.21 shows the model summary of the regression analysis indicating the R-value and R-square values to be 0.816 and 0.666. This shows the presence of high correlation between the independent variable data transformation, and dependent variable cybersecurity measures. Further, the R-square value indicates that data transformation can explain 66.6% of the total variation in cybersecurity measures.

Table 4.21: Model Summary

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.816[a]	.666	.664	2.50026	.666	394.961	1	198	.000

a. Predictors: (Constant), Avg_var5

b. Dependent Variable: Avg_var6

Table 4.22 shows the significance value of the regression model, where the significance value is 0.000 which is below 0.05. This explains that the model is a good fit for the data as it significantly predicts the outcome variable.

Table 4.22: ANOVA

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2469.023	1	2469.023	394.961	.000[b]
	Residual	1237.757	198	6.251		
	Total	3706.780	199			

a. Dependent Variable: Avg_var6

b. Predictors: (Constant), Avg_var5

Table 4.23 shows the coefficients table, where the significant value for data transformation is 0.000, which is below than 0.05. With 1% increase in the adoption of data transformation, the cybersecurity issues can rise by 1.202%.

Table 4.23: Coefficients

Coefficients[a]

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
	B	Std. Error	Beta			Lower Bound	Upper Bound

1	(Constant)	5.041	1.035		4.870	.000	3.000	7.082
	Avg_var5	1.202	.060	.816	19.874	.000	1.083	1.321

a. Dependent Variable: Avg_var6

Thus, the result indicates that the null hypothesis is rejected as significant recommendations can be determined because of the existence of significant relationship between the variables.

4.6. Chapter Summary

The ‘Results’ chapter focuses on analyzing the evaluated quantitative data from primary sources to explore the data protection issues with the adoption of digital transformation in SMBs, especially in context of Oman. The chapter involves explaining the research objective, data collection techniques, and tests hypotheses.

Further the chapter focuses on discussing the demographics of the participants from different SMBs in Oman who participated to complete the survey. The chapter employed statistical tests such as frequency of participant`s demographics indicating the exact percentage of their age-group, role, industry, and experience. Further, the chapter determined the Cronbach-alpha value to identify the credibility and validity of the overall gathered quantitative data, and descriptive statistics to determine the mean and standard deviation value to determine whether the data is dispersed.

The chapter then evaluated the results based on the null hypothesis and alternative hypothesis using several statistical tests such as correlation, one-sample t-test, one-way ANOVA, and regression analysis to address the three hypotheses. For hypothesis 1,

Pearson correlation test was performed to determine the relationship between the variables. For hypothesis 2, one sample t-test and one-way ANOVA was performed to determine the impact of the variables. And for hypothesis 3, regression analysis was performed to determine the relationship between the dependent and independent variables. The result for all the 3 hypotheses indicated that the null hypotheses was rejected while accepting the alternative hypotheses.

The next chapter of the research involves the 'Discussion' that involves discussing the primary findings by aligning with the scholarly sources based on research questions to effectively understand the impact of data protection and data-related issues with the adoption of digital transformation within SMBs, especially in Oman.

CHAPTER V:

DISCUSSION

5.1 Overview of Chapter

This chapter is a detailed and comprehensive overview of the results chapter which offers the reader a clear and better understanding of the data-related issues and data protection with the adoption of digital transformation especially within SMBs. The chapter focuses extensively on discussing the primary results to help understand the demographics, reliability, and descriptive statistics in a detailed manner. The study further discusses the research questions comprehensively by aligning them with the scholarly sources. Discussing the primary findings by aligning them with the scholarly sources help develop a better knowledge of adopting data transformation within SMBs. This further aids in determining a detailed discussion of the research questions that help understand the data-related issues mainly faced by organisational management as a result of technical progress, and inadequate security. Additionally, this chapter also discussed extensively on the recommendations that assists in reducing the issues of cyber security threats within SMBs. Thus, this chapter sheds light on the experiences of the participants gathered by conducting a survey on the adoption of digital transformation and its impact on data protection within SMBs in Oman. This further enables the researcher to compare and understand the primary findings from the secondary findings discussed in chapter 2.

5.2. Discussion of demographic questions, reliability test, and descriptive statistics

The results of demographic findings suggested the different views of Omani people on the adoption of digital transformation and data protection and security issues. The results firstly focused on discussing the age-group of the participants (table 4.1) that encapsulates a healthy proportion of participants with different age-groups who have taken part in the study, where the ratio of participants belonging from age-group 18-25 years is 24%, participants belonging from 26-35 years is 20.5%, and participants belonging from age-group 36-45 years is 20%. However, a smaller proportion of

participants belonging from the age-group above 60 years is 17% has participated to contribute to the research study.

Further, the frequency (table 4.2) highlights the role of the participants within their organisation. The results indicated that participants with different roles were asked to participate in the survey. A large proportion of participants who were data managers and play other roles in the organisation with 24% and 22% participated effectively. A similar proportion of participants who were IT managers and Security managers also participated with a ratio of 19%. However, a smaller proportion of participants who were the founders of their organisation also participated in the survey with a ratio of 15%. Gathering information from participants from different roles provided vast knowledge of the research context.

The primary demographic results further emphasised on discussing the industries from which the participants have come from. The results (table 4.3) showed the percentage of participants coming from different industries. Participants from diverse industries such as technology, healthcare, finance, retail, and manufacturing were approached to contribute to the survey. The findings explained that a large percentage (27%) of the participants were from the finance industry while 20% participants were from the healthcare industry, and 19% were from the technology and retail industry.

However, only 14% participants were from the manufacturing industry who contributed to the research. These participants operate their organisation in different ways and understand how the customers` data are impacted and what can be done to address the issues related to data.

The results further focused on the working experience of the participants. It is clear from table 4.4, that all the participants who have contributed to the study are experienced, however, the level of experiences of the participants varies. The primary results indicate that a large percentage of participants 26% had experience of more than 5 years, while 23.5% participants had more than 10 years. Participants with low experience level with percentage 16.5% & 11.5% had more than 15 years and 1 year of experience. This indicated that the participants with higher percentage of experience level provided

valuable insights to understand the data protection and security issues with the adoption of digital transformation, especially within SMBs.

After the demographics table, the research further focuses on discussing the determined reliability and credibility of the gathered data based on the study's objective. Firstly, the reliability and validity for the entire data has been determined. The Cronbach-alpha value (table 4.5) is determined to 0.921, which explains that the questions to conduct the survey are highly reliable and valid at the same time. Further, the primary findings of the reliability tests also determine the value for Cronbach-alpha if item deleted value (table 4.6), which is below 0.921 explaining that if any of these questions are deleted, it would not result in improving the reliability and credibility of the questions. However, the values for Cronbach-alpha if items deleted for 5 questions are greater than 0.921, explaining that if any of these 5 questions are deleted from the entire questionnaire, it would result in enhancing the value of Cronbach-alpha.

Further, the reliability and credibility of the questions under objective 1 has been determined. The Cronbach-alpha value (table 4.7) is determined to be 0.934, explaining that all the questions under this objective are highly reliable and credible. As the Cronbach-alpha value is greater than the decision value 0.6, the gathered data is considered as reliable and valid. Further, the primary results highlighted the values for Cronbach-alpha if item deleted (table 4.8). The results indicated that all the values for Cronbach-alpha if items deleted for all the 10 questions under objective 1 were below 0.934, explaining that if any of these questions were deleted from objective 1, it would not result in improving the Cronbach-alpha value for objective 1.

Table 4.9 shows the reliability and validity for the questions under objective 2. The primary findings determined the Cronbach alpha value to be 0.596 which is below 0.6 (table 4.9). As the determined Cronbach-alpha value is near to 0.596, it can be considered likely to be valid and credible. Further, table 4.10 highlights the Cronbach-alpha if item deleted values for all the questions under objective 2. The results indicated that all the values for Cronbach-alpha if items deleted under this objective are below 0.596, explaining that if any of these questions are deleted, it would not result in

improving the reliability and validity of the questions under this objective. However, only 1 question under this objective has a higher value for Cronbach-alpha if item deleted, explaining that if this question is deleted from objective 2, it would result in enhancing the Cronbach-alpha value for the objective.

Further, table 4.11 shows the reliability and validity of the questions under objective 3. The results from the primary findings determined the Cronbach-alpha value to be 0.930, explaining that all the questions under this objective are highlighted as reliable and credible as the reliability value is much higher than the decision value 0.6. Further, table 4.12 shows the value for Cronbach-alpha if the item deleted for the questions under this objective. The results indicated that the values for all the questions are below 0.930, explaining that if any of these questions from this objective are deleted, it would not result in improving the Cronbach-alpha value for the questions under this objective.

After the reliability and validity of the entire questionnaire has been determined, the primary results have further examined the descriptive statistics of the questions under each objective. The descriptive statistics explains the maximum and minimum value. Additionally, it also determines the mean, standard deviation, skewness, and kurtosis values for each question under each objective. The primary descriptive statistics results for objective 1 (table 4.13) shows the maximum value to be 5 and minimum value to be 1. This indicates that 5 is the most significant observation for the questions under this objective, and 1 is the smallest observation for each question under the objective. Further, the mean values for all the questions under the objective is determined to be close to 4. This explains that all the questions under this objective are closely related. Further, the descriptive statistics also show the value of standard deviation which explains the dispersion of data. The standard deviation values are determined to be between 0.8 and 0.9, indicating that the values are close to the mean value determined for the questions. This explains that the gathered data is highly spread out. Further, the skewness, and kurtosis values are also determined for the questions indicating the distribution of the shape and its peakedness. The results indicated a negative skewness for all the questions

under objective 1, which explains that the shape of the distribution is skewed to the left; and positive kurtosis value explains that the distribution of the shape has heavier tails. In other words, the peakness of the distribution is higher, when the value of kurtosis is higher.

The primary results for descriptive statistics for objective 2 (table 4.14) indicates the maximum and minimum value to be 5 and 1, explaining that 5 is the most significant observation and 1 is the smallest observation considered for the questions under objective 2. Further, the results of descriptive statistics determine the mean value to be between 2 to 4, indicating that the values are related and the values for standard deviation lie between 0.5 to 1. This also explains that these values are close to the mean values, which further determines that the data is highly spread out. The results further determined the skewness and kurtosis values for each question under objective 2, indicating the distribution of the shape and its peakedness. The results indicated a negative and positive skewness indicating that the distribution of the shape is skewed to the right and left. And the kurtosis value is also positive which explains the peakedness of the distribution of the shape.

5.3 Discussion on Research Question 1

As the research emphasises on examining the impact of digital transformation on the data-related issues, this section discusses the results of Pearson Correlation test which determines the relationship between the implementation of digital transformation, and the data-related issues within SMBs. The primary results determined by performing Pearson correlation test (table 4.16) determines a correlation value of 0.862, indicating the existence of strong relationship between the adoption of digital transformation and data-related issues within the SMBs. As the correlation value is positive and is also close to 1, it can be discussed that there is a strongly positive relationship between the implementation of digital transformation and data-related issues. The primary results can further be explained with the help of scholarly studies that discuss the impact of digital transformation on the data-related issues by determining the relationship between the two.

Implementation of digital technologies has transformed the world of businesses offering them various opportunities as well as issues. The adoption of digital technologies within SMBs has posed significant challenges, especially during the outbreak of the pandemic due to which SMBs have to adopt cloud technologies, e-commerce, online payment systems (Muthuraman et al., 2021). While other studies determined an increased number of benefits and opportunities with the implementation of digital technologies. With increased demand of customers to adopt digital technologies, SMBs have to shift themselves in order to grab the customer base. Additionally, this also results in increased employment within SMBs (Busaidi et al., 2022).

With a focus on Oman Vision 2040, the government has emphasized on driving the economic transformation with the adoption of advanced digital technologies. For this the government also focused on implementing several initiatives like the National Commerce for Digital Transformation, and Invest Easy, offering SMBs to have financial incentives and regulatory support to adopt digital transformation effectively in order to have a positive impact of digital transformation on the issues related to data, especially in SMBs (Al Balushi, 2019). Additionally, the implementation of digital technologies resulted in empowering and redefining the experiences of customers and the internal operations of the business, this indicates positive impact of digital transformation on the SMBs. However, negative impact of digital technology within SMBs has also been determined as the sudden outbreak resulted in rapid shift towards the technology due to which the organizational management did not have proper knowledge of implementing the technology. Additionally, the sudden implementation also resulted in restricted infrastructures and resources limiting the ability of the SMBs to gain competitive advantage. Hence, the business needs to adopt significant solutions that help streamline the business operations (Oladimeji and Owoade, 2024). Despite offering so many opportunities and benefits, the adoption of digital technologies results in data security issues within SMBs. This causes businesses to face issues such as data breaches, cyber security threats, and compliance with evolving regulations further leading to technical resources and limited financial issues. This indicates that the business has a negative

impact on the adoption of digital transformation and hence requires innovative solutions to address these digital vulnerabilities (Papathanasiou et al., 2024).

Adopting digital technologies results in negatively affecting the SMBs as it affects the prosperity and stability of the company. Digital transformation offers businesses the risk of cyber threats due to which sensitive information of customers are easy targets for attackers. Malware, phishing attacks, and ransomware are some of the most common attacks. Because of the financial restrictions and limited technical resources, SMBs mostly have to suffer from these data-related issues (Tekicand Koroteev, 2019b). In addition to this, financial constraints within SMBs also leads to devastating consequences which leads to major issues of data backup and recovery plans. SMBs also have to face issues which result in affecting inadequate data backup systems due to which there are issues of data losses. This determines the need to implement robust backup systems for data which ensures that the data is stored in a protected device and can be prevented from getting leaked in uncertain situations (Kumar, 2023).

Network security vulnerabilities are other challenges faced by Omani SMBs that arise due to unauthorized systems, weak firewalls, and unsecured Wi-Fi networks. These vulnerabilities are harmful for the SMBs which leads to susceptible to unauthorized access and cyberattacks. Because of these flaws within the SMBs, attackers can easily target the data and take advantage by entering into the internal networks. This enables them to hack all the sensitive data of the SMBs. Additionally, this further affects the budget of the SMBs due to which the organization is exposed to issues such as financial losses, data breaches, and reputational damage. Not only this, but SMBs also determine flaws in order to access control to authorize people (Corbett-Wilkins et al., 2023). Additionally, not adhering to data protection regulations also offers additional issues, especially in Omani SMBs. This results in leading to the loss of reputation within the organization further making it difficult for organisations to operate smoothly without having the risk of data vulnerabilities. Restricted financial budgets also enhance the chance of weak data security resulting in supply chain attacks further affecting the trust of customers and resulting in legal penalties (Ilori et al., 2024).

Because of the negative impact of digital transformation on the data-related issues, the organisational readiness of the SMBs have also been affected largely. This is so because being small businesses, SMBs are not much familiar with the adoption of digital transformations within their business operations which restricts them to have better hands-on experience and hence, SMBs find it challenging for them to function smoothly while ensuring that the customers` data are protected. Additionally, organisations also gather sensitive information from its employees which also needs to be protected and secured, however, limited digital transformation and hands-on experience can result in increased complications and quite costly for the SMBs to secure the confidential data of the employees and customers (Omrani et al., 2023). Not only this, but the scholarly sources have also explored the risks to flaws in access control which restricts access to authorize people which negatively affects the implementation of digital transformation within SMBs. The flaws in access to control mainly results in the leakage of data unintentionally. Additionally, this also leads to another vulnerability that leads to unpatched software and outdated systems which allows the hackers with the license to exploit the security and confidential data within the company (Ngonga et al., 2019).

Overall, the primary and secondary findings concluded that as the relationship between the data related issues, and digital transformation is strongly positive, it determines that there is a significant impact of digital transformation on the data-related issues within SMBs. Thus, it can be said that the null hypothesis is rejected.

5.4. Discussion on Research Question 2

The research question 2 focuses on examining the significant data-related challenges faced by the organisational management as a result of inadequate security and technical progress. Thus, to determine the challenges related to data faced by management as a result of technical progress and inadequate security, the research has performed one sample t-test, and one-way ANOVA which aided in determining the significant challenges faced by the SMBs, especially in Oman. The primary findings of the one sample statistics (table 4.17) determines the value of mean, and standard deviation for the questions. The mean values for the questions are close to 4 indicating

that the data are closely associated, and the standard deviation values are between 0.8 to 1 indicating that the data is highly spread out. Further, table 4.18 shows the result for one sample t-test indicating the significance value and the t-test value. From the results, it can be clearly discussed that the insufficient data storage, inadequate data security, complexity in data compliance with regulatory requirements, lack of data integration, lack of resources and expertise, lack of technical knowledge, and limited analytics capabilities are some of the challenges that the management face as a result of inadequate security and technical progress. This can be said so as the significant value is determined to be below 0.05. Further, the t-test value is also determined to be much higher from 1.96 explaining that these challenges have a significant impact in the SMBs due to technical progress and inadequate security.

The primary results further performed a One-way ANOVA test to assess the statistically significant difference between the data-related challenges and technical progress and inadequate security. As the results of the ANOVA tests (table 4.19) determine the p-value to be less than 0.05, it indicates that there is a statistically significant difference between the means of the data-related challenges, and technical progress and inadequate security. In other words, this helps in understanding the statistical difference between the means of the data-related challenges, and the technical issues, and inadequate security.

The primary results can further be explained with the help of scholarly studies that discuss the data-related challenges faced by organisational management as a result of technical progress and inadequate security.

The adoption of digital transformation has been largely implemented within Arab countries, especially during the pandemic in order to operate businesses when other businesses were shutting down. Hence, businesses shifted largely towards digital transformation, however, the sudden shift towards digital transformation resulted in various data-related issues causing protection and security issues with customers` and employees` data. These issues result in cyber security vulnerabilities, resistance to change, and compliance issues at the same time. The technical progress within the digital

technologies further resulted in improving the customer relationship management, however, the issues of cybersecurity threats and data breaches have still been one of the most unaltered issues within SMEs (Alkhattali, 2025). Similarly, when advanced digital technologies were adopted largely in the Arab Gulf Region, mainly in Saudi Arabia, it emphasised on implementing UAE`s Smart Government Strategy which resulted in accelerating the accounting process and offering businesses with enhanced efficiency and capability of making decisions at the same time. However, businesses not only experienced benefits from implementing digital technologies within their operations but were also exposed to several major cybersecurity threats that included issues related to ransomware, insider attacks, and phishing attacks. This resulted in affecting the trust of customers and the employees within the companies (Morshed and Khrais, 2025).

Different digital technologies such as big data analytics, and cloud computing have been adopted largely within SMBs in order to improve the business performance. As these technologies have been largely implemented within businesses, it has resulted in affecting the environmental, organisational, and technological contexts. These further result in impacting the financial and marketing aspects of the businesses which is quite challenging for them. The financial constraints result in posing significant threats and risks to customers' data privacy which puts a strain on the back-end support systems. This results in increasing the traffic on networks which allows businesses to use conferencing and collaboration services (Maroufkhani et al., 2020). Furthermore, when SMEs focus on adopting cloud computing from providers, they often have to face difficulties based on their business continuity strategies. This results in arising questions if public cloud architecture can effectively deliver services even when the staff services are not working to determine the robustness, and scalability of handling the rising demand of the technology. Infrastructure constraints must be addressed robustly to ensure access to public cloud services and to handle the rising traffic volumes. This helps in the management of risks and uncertainties while handling unexpected spikes in the demand of the technology. Additionally, this increased demand results in exacerbating the remote work, streaming services, and substituting the digital events for in-person meetings.

Further, the cloud providers are also impacted by the supply networks that result in shortages further leading to stress of not handling the dangers that occur due to the implementation of cloud computing (Mandal and Khan, 2020).

Ransomware is another significant major issue that occurs within SMEs with the adoption of digital transformation. This is a virus that holds the data hostage in exchange for money. This issue results in avoiding the conventional backup procedures due to which the malware iteration gets access to the association data which ends in backing up the data and the ransomware virus. This makes it difficult to return back to the optimal form of data which can be managed only when the vendors try to manage and modify the backup and recovery products so that the novel ransomware capabilities can be managed effectively. Additionally, these risks result in increasing the chances of making employees feel less protected, especially when they use insecure networks. However, these issues can be addressed effectively by CDM which helps lowering the data to store, manage, and protect it efficiently (Doyle at al., 2020).

In contrast to the above studies, significant gaps have been identified in data security and inadequate technological advancements which exposes Omani FinTech SMEs to face financial instability and operational risks in the management of data. With a focus on addressing these gaps, SMEs often require advanced detection systems, enterprise-wide security strategies, and effective regulatory frameworks that are helpful in eradicating these threats. Additionally, these gaps can also be addressed with the help of a continuous monitoring system that allows businesses to mitigate cyber security risks. This further helps businesses to equip with innovative solutions that aids in strengthening the cybersecurity measures, safeguarding operations, and enhancing data protection that effectively help evolve the digital landscape (Webb and Sallos, 2024). Not only this, but the absence of dedicated IT security teams is also one of the major reasons that are exposed to gaps in data security, however, when an adequate IT security team is involved within the SMEs with better hands-on experience, along with their expertise that enables them to mitigate these risks. Post-pandemic most of the organisations faced financial constraints due to which they were exposed largely to digital vulnerabilities such as cyber

security threats. This further led to an increased issue of data breaches that are caused due to phishing attacks, and ransomware attacks. This determined significant issues such as lack of skilled personnel, structured processes, and planned IT budgets which is effective in bridging the security gaps within SMEs and large companies (Heidt et al., 2019).

In contrast to this, in order to be competitive, SMEs have been largely adopting innovative digital technologies that results in eradicating the challenges that occur due to the adoption of advanced digital technologies. Because of lack of hands-on experience and knowledge about the implementation of digital technologies, there is an increase in the rise of cybersecurity threats within SMEs which have made these organisations main targets for the cyber criminals. The main reasons why cyber criminals target these organisations are because of limited resources, insufficient security budgets, lack of trained personnel, and inadequate awareness of cyber risk exposure. Further, to address these gaps within the SMEs, significant cost-efficiency and security measures are required which involves the deployment of security-as-a-services to secure a high level of security for the organisations especially when they face financial constraints. Additionally, the development of security culture within the organisation can also be done along with providing multi-factor authentication to minimise the issues of cyber security threats (Tejada, 2020).

Overall, the primary and secondary findings concluded that as the significance value for data-related challenges as a result of technical progress and inadequate security have been determined, this results in impacting the management adversely. Thus, it can be said that the null hypothesis is rejected.

5.5. Discussion on Research Question 3

The research question 3 emphasises on identifying the recommendations that assists in reducing the cyber security threats within SMBs in Oman. Thus, to identify the recommendations addressing cybersecurity issues, the research has performed Pearson correlation and regression analysis to determine the relationship between the digital transformation and cybersecurity measures that can be considered to address the issues. The primary results determined by performing Pearson correlation test (table 4.20)

determines a correlation value of 0.816, indicating the existence of strong relationship between the adoption of digital transformation and cybersecurity threats within the SMBs. As the correlation value is positive and is also close to 1, it can be discussed that there is a strongly positive relationship between the implementation of digital transformation and cybersecurity threats.

Further, the research has also performed the regression analysis (4.21) showing the table of model summary which indicates the value of R and R-square. The R-value is determined to be 0.816 indicating a strong and positive association between digital transformation and cybersecurity threats, and R-square value is determined to be 0.666 which discusses that digital transformation can explain 66.6% of the total variation in cybersecurity measures. Further, table 4.22 indicated a significance value of 0.000 explaining the regression model to be a good fit for the data. And table 4.23 shows the unstandardized coefficients explaining that 1% increase in implementing digital transformation can result in increasing cybersecurity measures by 1.202%.

The primary results can further be explained with the help of scholarly studies that discuss the recommendations that assists in reducing the cyber security threats within SMBs in Oman.

Industry 4.0 has employed advanced technologies within its business operations that has impacted the businesses largely either by replacing jobs, or by increasing the productivity of the workers or by enhancing workplace safety. The increased adoption of digitisation has offered various innovative solutions which has made costs fall down by ensuring that the businesses prevent themselves against any attacks. Considering this Disaster Recovery as a Service (DRaaS) is one of the most popular services that are used by the businesses with the most critical systems where the organisations keep duplicated data instead of backing it up. This further enables converting the data from traditional paper-based processes to digital formats which allows to have a more effective computer-assisted information management. Incorporating innovative digital solutions brings transformative change within the businesses with a focus on increased consumer accountability, and improved business process efficiency. Further, businesses and firms

should also emphasise on redesigning the business models especially when they have restrictions related to digital divide, organisational firmness, and unequal effects on worker prosperity, however, these can be dealt with the availability of user-friendly digital technologies, reduced costs for digital data storage, and potential proficiency gains that effectively aids in cost savings and better time management offering employees and staffs with the flexibility of working from home.

In addition to this, the Omani government should also emphasis on establishing financial incentives and effective policies that offer organisations with the capability of transitioning towards digitisation and earn profits in the longer term. This also enables customers to develop trust within the organisation as the sensitive data provided by them to the organisation while making transactions or purchasing products is safeguarded and are not at risk of cyberattacks. Thus, the need for developing technological infrastructure can effectively promote access and offer traditional communities within the businesses with digital technology implementation. This further offer businesses with a foundational support which allows businesses to take advantage of these technologies by enhancing its openness in corporate operations and also helps the business in its cost and productivity standards.

Automation is another effective strategy that can be highly considered within the businesses, especially during the times of the Coronavirus outbreak. Considering these initiatives within business operations can result in immediate return on investment by automating specific work processes and saving time on manual tasks. Additionally, HRs and other employees within businesses can also get more time to focus on data-related issues by redeploying themselves to fill-in for basic deficiencies within the businesses. And to manage these deficiencies, businesses can effectively use more advanced machine learning tools and technologies. However, the businesses in the post-pandemic era still remained competitive with the continuous implementation of digital technologies that further aids businesses in enhancing their resilience and competitiveness within the market. Government can also emphasis on accelerating efforts that help in transitioning the digital age by enhancing financial, regulatory, and advising assistance for companies,

especially when they lack digital competence by allowing the access to high-speed internet and broadband infrastructure connectivity within the businesses.

Further, significant recommendations have also been made for cyber threats within businesses. SMBs mainly focus on implementing ERP systems that aid in automating planning, inventory control, and corporate operations that work on computer-based systems. These can effectively help in managing and organising the flow of information from both ways internally and externally with a focus on finance and sales. RFID or radio frequency identification technologies are other effective tools which when implemented within SMBs can help in redesigning the logistics and manufacturing efficiency. Along with this, this software also aids in supply chain operations and front office integration that mainly helps improve customer relationship management.

Businesses also use cloud computing that are quite helpful in improving and upgrading the IT infrastructure by preventing customer`s data and sensitive information against cyberattacks. These advanced digital technologies offer SMEs the opportunity to access databases software, and also offers additional storage capacity in large amounts by aligning and adhering to the demands of the SMEs. As this technology is highly adaptable and scalable, it leads to lower the technology cost by redesigning and relieving businesses with customary costs and open hardware investments. Similarly, big data analytics is another significant recommendation that can be implemented within SMEs to protect the sensitive information from attackers. Implementing this technology not only increases productivity in marketing, advertising, and commercialisation but also offers effective strategic planning, decision-making, pre-production, logistics, administration, and manufacturing that aids in analysing large amounts of data produced by electronic and machine-to-machine interactions. This also helps in enhancing their consumer base and improve their brand awareness.

Overall, the primary and secondary findings concluded that as the relationship between the digital transformation and cybersecurity threats is strongly positive, it determines that there is a significant impact of digital transformation on the data-related issues within SMBs. Additionally, the primary results also determined that an increase in

the adoption of digital transformation leads to increased cybersecurity threats. Thus, it can be said that the null hypothesis is rejected.

5.6. Summary of Chapter

The chapter summarizes the findings determined by performing statistical tests with the help of the statistical software SPSS. By aligning with the research objectives and questions the statistical tests were performed and the results were presented in the previous chapter. However, this chapter discusses those results explaining the main findings in a more detailed manner. This enables to understand the data-related issues within the SMBs and its impact on the organisation. Along with this, the study also helps in understanding the significant recommendations that are effective in addressing the data-related issues within the SMBs.

Firstly, this chapter discussed the impact of data-related issues with the implementation of digital transformation by determining the relationship between these which also explains the impact of the issues on the adoption of the technology. The findings rejected the null hypothesis by explaining the significant impact of data-related issues on the implementation of digital transformation. In addition, scholarly articles were also discussed explaining the impact of the data-related issues on the implementation of digital technologies.

Secondly, the chapter discussed the data-related challenges faced by the SMBs as a result of technical progress and inadequate security. And to determine this, one-sample t-test and one-way ANOVA tests were performed. The primary results identified the issues by rejecting the null hypothesis which discussed the issues related to data with the implementation of digital technologies within the businesses. Further, the secondary findings from the scholarly sources also discussed the data-related issues faced by the organizational management when the businesses shifted towards digital technologies.

The chapter then discusses the recommendations that assists in reducing the cybersecurity threats and minimise data-related issues. To identify the recommendations, the researcher has performed the regression analysis to identify the relationship between the dependent and independent variables to further identify whether the model is a good

fit to determine the recommendations. The key findings further discussed that the identified recommendations can effectively assist in reducing the cybersecurity threats and issues while rejecting the null hypothesis. Further, the secondary findings with the help of scholarly sources also discussed recommendations that address cybersecurity threats within SMBs.

CHAPTER VI:
SUMMARY, IMPLICATIONS, AND RECOMMENDATIONS

6.1.Summary of Chapter

The sudden emergence of COVID-19 pandemic has led the business world shift towards digital transformation offering customers and businesses a novel approach of

shopping and running their businesses. The increased implementation of digital technologies within SMBs has further resulted in increased risks of data privacy and security concerns. As the small and medium-sized businesses in the Sultanate of Oman have also implemented digital technologies within their businesses, it has also been exposed to several major risks and data threats, which is one of the major challenging issues for SMBs to lose their customers and ultimately find it difficult for their business to operate smoothly.

Considering this as an important area to research and address the research objectives, the study has effectively formulated hypotheses based on the objectives of the research and also by aligning with the research questions. Thus, the first hypothesis emphasises on analysing the correlation between the data-related issues and the implementation of digital technologies. The findings from primary statistical analysis along with the secondary analysis has determined a significant impact on the implementation of digital transformation. Thus, the first hypothesis states that the null hypothesis is rejected, explaining a robust positive relationship (r=0.862) between the data-related issues and digital transformation. The secondary analysis from the literature review also provided a deep understanding of the impacts of data-related issues with the adoption of digital transformation.

The study then emphasised on the second hypothesis by aligning with the research objectives and questions. This hypothesis focuses on identifying the significant data-related challenges within the business management as a result of technical progress and inadequate security. To test the hypothesis, the impact of the data-related issues on technical progress and inadequate security has been determined. It has been found out that there is a significant positive impact of the data-related challenges due to technical progress and inadequate security, as the significant value is 0.000. The study further depicts that the results and discussions chapter explains that inadequate security and technical progress within the digital technologies leads to increased issues related to data.

Further, the researcher has emphasised on the third hypothesis by aligning with the research objectives and questions, where the hypothesis aimed at determining the

significant recommendations to address the rising issues of cybersecurity threats within SMBs. In order to test the hypothesis, the study performed the regression analysis, and the key findings from the results chapter determined (R^2 = 0.666, F=394.961, and p-value = 0.000) highlighting the significant recommendations that are important in managing and reducing the cybersecurity threats. With the implementation of complex technologies, SMBs largely require training sessions for the staff and employees, advanced infrastructure, improved knowledge and expertise which are important to facilitate the implementation of digital transformation within SMBs.

6.2. Implications

The shift towards digital transformation has offered the business world numerous benefits and advantages and has played a significant role in transforming the way of business operations while ensuring that the customers` data are safe with the organisation. Focusing on this, the researcher has emphasised on defining the theoretical and practical implications for the current research. The theoretical underpinnings of implementing digital transformation in Omani SMBs depicts increased issues related to data breaches, leakage, cybersecurity attacks, threats, and data vulnerability. Considering the theoretical implications as important, theories such as Technology Acceptance Model, Risk Assessment Framework and GDPR Framework enables the researcher to gain an in-depth understanding of the data-related issues and its impact on the digital transformation within Omani SMBs and the strategies required to address the issues. While the practical implications of the findings will aid in empowering the employees, staff, and business owners of the Omani SMBs to gain increased knowledge and understanding towards the shift of digital transformation, data-related issues that occur due to this shift, and the recommendations that can be considered effective to address these issues. Thus, these implications will guide the researchers in future about the data-related issues along with the strategies to address these in Oman.

6.2.1. Theoretical Implications

From the Technological Acceptance Model, it has been clearly understood that the technologies are largely accepted within the businesses. Davis, in his model explained

that the adoption of technologies within businesses requires to be equipped with enhanced knowledge and understanding of the significant factors. Thus, this theory of knowledge offers a vast understanding of the technologies that are to be implemented within the business, further offering SMBs in Oman to adopt the digital transformation largely. This implementation resulted in making businesses adopt the advanced technologies to have numerous benefits and advantages which empowers business owners, employees and staff to develop effective strategies while ensuring to protect the data and sensitive information provided by the customers.

Further, the Risk Assessment Framework developed by the US government emphasized largely on the protection and prevention of sensitive information and data. Considering this, the framework worked by setting up guidelines by identifying, eliminating, and minimising the data-related risks. As the SMBs in Oman adopted this framework, they can easily emphasize on navigating the data-related threats and risks involving IT issues, litigation issues, loss of capital. As eliminating these risks is not easy, this framework enables SMBs to mitigate these and aid in running their business efficiently by involving the main components such as identification, measurement, assessment, mitigation, reporting, monitoring and governance. This further allows businesses to effectively identify and eliminate the data-related risks.

The GDPR framework is another effective framework used in the current research which offers SMBs with robust requirements that aids in processing personal data and information without complying with the adjustment protocols. The GDPR regulations focus largely on enabling organizations to achieve compliance by protecting and safeguarding against cyberattacks, data security and privacy. For this, the framework offers legal frameworks, valid data encryption methods and data acquisition policies. The framework further emphasises on differentiating the ethical, and legal challenges that effectively aids in deploying defensive data management strategies to offer its customers with justice and certainty while informing about the different cybersecurity and privacy issues.

6.2.2. Practical Implications

The shift towards digital transformation has profound significant practical implications for the SMBs in the Sultanate of Oman. This shift has resulted in storing large amounts of customers and employees data, making them vulnerable about the data and information that they shared with the SMBs, which in turn, results in loss of trust. Practically, the shift towards digital transformation leads to issues that affect the customers making them lose their personal information. Hence, the customers mainly purchase from organisations with better and improved advanced technologies. Further, this impacts the customer's view of purchasing from the same organisation due to data-related risks.

The adoption of digital technologies within the SMBs lead to increased data-related issues as a result of technical progress and inadequate security. As the digital technologies are largely adopted within SMBs in Oman, a large number of issues related to lack of resources, lack of infrastructure, financial constraints, and because of other reasons are also determined which results in exposing risks and threats to organisational data resulting in leakages and breaches. As the issues related data are identified, significant recommendations can be practically considered to address the cybersecurity issues powered by effective and advanced algorithms suggesting strategies, and methods through which data can be prevented and protected against cyberattacks. Recommendations such as offering training sessions to employees, staff, and business owners, financial assistance, improved infrastructure, better resources and other effective strategies can effectively aid in navigating the data-related issues with the implementation of digital technologies within SMBs.

6.3. Recommendations for Future Research

By understanding the implications of the study, the following suggestions are recommended for future research when researching to explore data protection and security after the businesses shift towards digital transformation.

The availability of existing studies on the implementation of digital transformation in SMBs in Oman are only few, which requires an increased number of studies in this specific area. As the demand for digital transformation has risen, the rate of

shifting towards technology could also be higher. Thus, this requires an increased number of studies on this topic so that the management of SMBs can also be aware of the advantages and the issues, which might be helpful for them to bring efficiency to the research outcomes.

As digital transformation has been considered one of the most effective ways to operate business during the COVID-19 pandemic, it also demanded highly skilled workers with advanced infrastructure. Thus, it is significant for SMBs to invest largely on upskilling employees by offering training sessions to them and ensuring to avail advanced infrastructure which effectively aids in empowering business to shift effectively towards digital transformation.

The current research has emphasised on exploring the challenges related to data protection and security when SMBs adopt digital technologies. However, it is significant to discuss these challenges comprehensively in order to understand the factors that are important in ensuring the smooth integration of digital technologies within the SMBs.

The current study has followed a 5-point Likert scale for the survey questionnaire, however, most of the studies use a 7-point Likert scale that helps in analysing the answers in a more detailed manner. Thus, choosing a 7-point Likert scale would be effective when conducting future research as it would be more convenient for the participants to express their agreement and contribute to the findings.

The current study only involved independent and dependent variables. However, further studies can also consider exploring the moderating variables along with the likelihood of the existence of external variables that results in affecting the implementation of digital transformation within SMBs.

6.4. Conclusion

The current study highlighted the background and rationale of shifting towards digital transformation while exploring the issues and challenges related to data within SMBs within the Sultanate of Oman. The main aim of this study emphasised on exploring data protection and security when SMBs shift towards digital transformation. Thus, the business invests largely in conceptualizing, developing, and executing effective

strategies to implement digital technologies smoothly within SMBs. As the SMBs in Oman have largely shifted towards digital transformations past-pandemic, the businesses have witnessed a large number of profits, however, this has also led to an increased number of challenges posing threats mainly to data-related issues.

Despite the challenges the SMBs in Oman have been investing in the implementation of digital transformations with a focus on earning more profits and expanding their business, but at the same time businesses also require strategic moves to attract customers by gaining the trust of the customers. Thus, the research study has emphasised on evaluating the views of business owners, employees, and staff within the Omani SMBs by conducting a survey. The results gathered from conducting the survey are presented in Chapter 4 'Results'. Apart from this, the chapter also provides a brief knowledge about the participants who participated in the survey explaining how the adoption of digital transformation has affected them and the data in the organisation.

The research further presents a comprehensive Literature Review from the academic literatures that are relevant in examining the data protection and security issues that occur within SMBs in the Omani context to effectively understand its impact on digital transformation. This section of the literature review provides a detailed understanding of what digital transformation is and how it is affecting the SMBs in Oman by effectively determining the benefits and issues that occur after the implementation of digital technologies. Further, the literature review chapter extensively discusses the challenges that occur with the adoption of digital technologies within the SMBs. The significant issues involve lack of expertise, lack of knowledge, training sessions, lack of resources, lack of infrastructure and others. Not only this, but the section also discusses the significant gaps. After this, the literature review chapter focuses on discussing the recommendations that can be considered effective in minimising the cybersecurity risks so that they can be eradicated. This section of the chapter comprehensively discusses the significant recommendations such as offering training sessions, gaining expertise, improving knowledge about the implementation of technology, and financial and

infrastructural assistance can help in navigating the cybersecurity threats and data breaches effectively.

The chapter further focuses on determining the significant knowledge gaps that are determined by exploring through the secondary scholarly sources. The critical knowledge gaps determined a lesser number of studies that have emphasised on the implementation of digital transformation and the data-related issues that lead to occur data protection and security concerns within the SMBs, especially in the context of Oman. Additionally, the existing studies have also been aligned with the theoretical and conceptual framework by further aligning with the research objectives and questions mentioned in Chapter 1 'Introduction'.

Further, the research involved discussing the appropriate research methods and processes that are required to conduct the study further. As the study has conducted a survey, it has selected a quantitative research method so that the researcher can use a statistical method to analyse the gathered data through the results of the survey. By involving a total of 200 participants who were the employees, staff, and business owners working within SMBs in Oman have participated in the survey by ensuring that they have at least 1 year of experience. Further, the gathered data has been analysed using the SPSS software to determine the results.

The research further tested the hypothesis based on the survey results after discussing about the participants, their age-group, industry they are working in, role in the organisation, and their level of experience. The research then tests hypothesis 1 by performing the correlation test and determining the relationship between the data transformation and data-related issues. The findings further determined a significant, robust and positive outcome that discusses the significant impact of darta-related issues in the implementation of digital transformation within SMBs. The findings have further also been supported by secondary sources that help in better understanding of the impact of digital transformation on data-related issues. It resulted in rejecting the null hypothesis and accepting the alternative hypothesis.

Further, the research tests hypothesis 2 by performing one-sample T-test and one-way ANOVA. The results of one-sample T-test also suggested a significant outcome by explaining that the challenges such as lack of expertise, knowledge, understanding, financial constraints, infrastructure, and other issues occur within SMBs. Further, the results from the ANOVA test determined the p-value to be less than 0.05 indicating a significant value suggesting the significant impact of the challenges on the organization. This resulted in rejecting the null hypothesis and accepting the alternative hypothesis. The findings have also been supported by secondary sources that help in better understanding of the challenges related to data.

The research further tests hypothesis 3 by performing the regression analysis. The result of the hypothesis explains that significant recommendations can assist in reducing the cybersecurity threats and data breaches. The results of the regression analysis determine the high correlation between the dependent and independent variable while determining the total variation in the cybersecurity measures. Further, this has also been supported by the scholarly articles which discusses the recommendations comprehensively. Overall, the null hypothesis for this objective has also been rejected while accepting the alternative hypothesis.

Thus, from all the above-discussed hypotheses, suggests a positive and robust relationship between the variables by rejecting the null hypotheses and accepting the alternative hypotheses for all the objectives.

REFERENCES

Adebayo, A., and Ackers, B. (2021) Sampling theoretically for comparison. Electronic *Journal of Business Research Methods*, 19(1), pp42-56. https://doi.org/10.34190/ejbrm.19.1.2434

Al Jabri, M.S.K. and Matriano, M.T. (2023) An empirical study on SMEs growth and sustainability: A Case Study in Oman.*GSJ*, 11(9), pp. 110–122. https://www.researchgate.net/profile/Manal-Al-Jabri/publication/373840711_An_Empirical_Study_on_SMEs_Growth_and_Sustainability_A_Case_Study_in_Oman/links/64fffeeef8931a4e29b94708/An-Empirical-Study-on-SMEs-Growth-and-Sustainability-A-Case-Study-in-Oman.pdf.

Al Sheibani, S.M.N. (2020) What determines and deters innovation in the British and Omani small and medium-sized enterprises -CentAUR.*University of Reading*.https://centaur.reading.ac.uk/97043/.

Alkhattali, M. (2025) Impact of digital integration on the Small and MediumSized Enterprises in Arab countries.*SSRN Electronic Journal* [Preprint]. https://doi.org/10.2139/ssrn.5147411.

Al-Maskari, A. *et al.* (2019) Internal and external obstacles facing medium and large enterprises in Rusayl Industrial Estates in the Sultanate of Oman.*Journal of Global Entrepreneurship Research*, 9(1). https://doi.org/10.1186/s40497-018-0125-3.

Alog, K. *et al.* (2025) Impact of Digital Integration on the Small and Medium-Sized Enterprises in Arab Countries.*AAJSR*, pp. 41–54. https://aajsr.com/index.php/aajsr/article/view/322.

Alriyami, S.N.S. and Ahmed, M. (2023) The use of technology among the Omani retailers amidst the COVID-19 pandemic.*International Journal of Business Performance Management*, 24(3/4), pp. 429–441. https://doi.org/10.1504/ijbpm.2023.132325.

Aslan, Ö. *et al.* (2023) A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions.*Electronics*, 12(6), p. 1333. https://doi.org/10.3390/electronics12061333.

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

Bahador, M.H. and Ibrahim, S.S. (2021) Technology Innovations toward Sustainable Growth of Small Medium Enterprise (SMEs): Aftermath COVID-19 Pandemic.*International Journal of Academic Research in Business and Social Sciences*, 11(2). https://doi.org/10.6007/ijarbss/v11-i2/9199.

Belwal, R., Shibli, R.A. and Belwal, S. (2020) Consumer protection and electronic commerce in the Sultanate of Oman.*Journal of Information Communication and Ethics in Society*, 19(1), pp. 38–60. https://doi.org/10.1108/jices-09-2019-0110.

Bitwize - (no date) Over 141,000 SMEs registered in Oman by the end of June 2024. https://timesofoman.com/article/150193-over-141000-smes-registered-in-oman-by-the-end-of-june-2024.

Cahyono, D. *et al.* (2025) Challenges and opportunities in implementing big data for small and medium Enterprises (SMEs).*Journal.corisinta.org* [Preprint]. https://doi.org/10.33050/zaz3sj02.

Chitra, M., Surianarayanan, R., Mahamuni, V. S., Mohammed, S., Keno, M. T., and Boopathi, S. (2024). Study on Cloud Computing-Empowered Small and Medium Enterprises. *In Advances in business information systems and analytics book series* (pp. 189–220). https://doi.org/10.4018/979-8-3693-4227-5.ch008

Coleman, S. *et al.* (2016) How Can SMEs Benefit from Big Data? Challenges and a Path Forward.*Quality and Reliability Engineering International*, 32(6), pp. 2151–2164. https://doi.org/10.1002/qre.2008.

Eltaeib, T., Abuzneid, S. and Elleithy, K. (2024) Proposed Framework for a Comprehensive Cybersecurity Risk Management Strategy.*IEEE Conference Publication | IEEE Xplore*, pp. 1–6. https://ieeexplore.ieee.org/abstract/document/10808119.

Habib, G. *et al.* (2022) Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing.*Future Internet*, 14(11), p. 341. https://doi.org/10.3390/fi14110341.

Heidt, M., Gerlach, J.P. and Buxmann, P. (2019) Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments. *Information Systems Frontiers*, 21(6), pp. 1285–1305. https://doi.org/10.1007/s10796-019-09959-1.

Hoofnagle, C.J., Van Der Sloot, B. and Borgesius, F.Z. (2019) The European Union general data protection regulation: what it is and what it means.*Information & Communications Technology Law*, 28(1), pp. 65–98. https://doi.org/10.1080/13600834.2019.1573501.

Klein, V.B. and Todesco, J.L. (2021) COVID-19 crisis andSMEsresponses: The role of digital transformation *Knowledge and Process Management*, 28(2), pp. 117–133. https://doi.org/10.1002/kpm.1660.

Kraus, S. *et al.* (2021) Digital Transformation: An overview of the current state of the art of research.*SAGE Open*, 11(3). https://doi.org/10.1177/21582440211047576.

Kshetri, N. (2017) Blockchain's roles in strengthening cybersecurity and protecting privacy.*Telecommunications Policy*, 41(10), pp. 1027–1038. https://doi.org/10.1016/j.telpol.2017.09.003.

Matriano, M.T. (2022) Global Challenges for business and entrepreneurship: Case of Oman.*Advances in Social Sciences Research Journal*, 9(1), pp. 419–425. https://doi.org/10.14738/assrj.91.11660.

Mishrif, A. and Khan, A. (2023) Technology adoption as survival strategy for small and medium enterprises during COVID-19.*Journal of Innovation and Entrepreneurship*, 12(1). https://doi.org/10.1186/s13731-023-00317-9.

Mokalled, H. *et al.* (2017) The Importance to Manage Data Protection in the Right Way: Problems and Solutions.*In Springer proceedings in mathematics & statistics*, pp. 69–82. https://doi.org/10.1007/978-3-319-67308-0_8.

Morić, Z. *et al.* (2024) Protection of personal data in the context of E-Commerce. *Journal of Cybersecurity and Privacy*, 4(3), pp. 731–761. https://doi.org/10.3390/jcp4030034.

Morshed, A., and Khrais, L. T. (2025). Cybersecurity in digital accounting Systems: Challenges and solutions in the Arab Gulf region. *Journal of Risk and Financial Management*, 18(1), 41. https://doi.org/10.3390/jrfm18010041

Nallakaruppan, M.K., Pethani, A. and Pelusi, D. (2025) Data Security in the Age of Marketing: Safeguarding customer information and compliance.*In Emerald Publishing Limited eBooks*, pp. 165–178. https://doi.org/10.1108/978-1-83662-326-720251022.

Piza, C. *et al.* (2016) The Impact of business support services for small and medium Enterprises on Firm Performance in Low- and Middle-Income Countries: A Systematic review.*Campbell Systematic Reviews*, 12(1), pp. 1–167. https://doi.org/10.4073/csr.2016.1.

Rawindaran, N. (2023) Impact of cyber security awareness in small, medium enterprises (SMEs) in Wales.*Figshare* [Preprint]. https://doi.org/10.25401/cardiffmet.23599497.v1.

Saeed, S. *et al.* (2023) Digital Transformation and Cybersecurity Challenges for businesses Resilience: Issues and recommendations.*Sensors*, 23(15), p. 6666. https://doi.org/10.3390/s23156666.

Schwertner, K. (2017) Digital transformation of business.*Trakia Journal of Sciences*, 15(1), pp. 388–393.

https://pdfs.semanticscholar.org/51bb/4fd609d174438fb8911f283d48d34ef1e894.pdf/1000.

Shandilya, S.K. *et al.*(2024) Navigating the regulatory landscape.In *EAI/Springer Innovations in Communication and Computing*, pp. 127–240. https://doi.org/10.1007/978-3-031-53290-0_3.

Taubenberger, S. (2014) Vulnerability identification errors in security risk assessments. https://doi.org/10.21954/ou.ro.00009aca.

Ulsch, N.M. (2014) Cyber threat*!*,*Wiley eBooks*. John Wiley & Sons, Inc. https://doi.org/10.1002/9781118915028.

Uvarova, O. (2021) SMEs Digital Transformation in the EaP countries in COVID-19 Time: Challenges and Digital Solutions.*EaP CSF COVID-19 POLICY PAPER*. report. https://d1wqtxts1xzle7.cloudfront.net/66211097/SMEs_digital_transformation_in_the_EaP_countries_during_COVID_19_1_-libre.pdf?.

Vial, G. (2021) Understanding digital transformation.In *Routledge eBooks*, pp. 13–66. https://doi.org/10.4324/9781003008637-4.

Wang, P. *et al.* (2019) Economic costs and impacts of business data breaches.*Issues in Information Systems* [Preprint]. https://doi.org/10.48009/2_iis_2019_162-171.

Wu, J. *et al.* (2024) Uncovering the dynamics of enterprises digital transformation research: A comparative review on literature before and after the COVID-19 pandemic.*Heliyon*, 10(5). https://www.cell.com/heliyon/fulltext/S2405-8440(24)03017-2.

Agrawal, P. and Narain, R., (2019) Digital supply chain management: An Overview. In *IOP Conference Series: Materials Science and Engineering* (Vol. 455, No. 1, p. 012074). IOP Publishing.

Ajibade, P. and University of KwaZulu-Natal. (2018) Technology Acceptance Model Limitations and Criticisms: Exploring the practical applications and use in technology-related studies, mixed-method, and qualitative researches. *In*

University of Nebraska - Lincoln & University of Nebraska - Lincoln, Library Philosophy and Practice (E-journal) [Journal-article]. https://core.ac.uk/download/pdf/189486068.pdf

Alsyouf, A., Lutfi, A., Alsubahi, N., Alhazmi, F. N., Al-Mugheed, K., Anshasi, R. J., Alharbi, N. I., and Albugami, M. (2023) The use of a Technology acceptance model (TAM) to predict patients' usage of a personal health record system: the role of security, privacy, and usability. *International Journal of Environmental Research and Public Health*, *20*(2), 1347. https://doi.org/10.3390/ijerph20021347

Amoo, O. O., Atadoga, A., Osasona, F., Abrahams, T. O., Ayinla, B. S., and Farayola, O. A. (2024) GDPR's impact on cybersecurity: A review focusing on USA and European practices. *International Journal of Science and Research Archive*, *11*(1), 1338–1347. https://www.researchgate.net/profile/Olukunle-Amoo/publication/378106122_GDPR's_impact_on_cybersecurity_A_review_focusing_on_USA_and_European_practices/.pdf

Angelini, M., Ciccotelli, C., Franchina, L., Marchetti-Spaccamela, A., and Querzoni, L. (2020) Italian National Framework for Cybersecurity and Data Protection. *In Lecture notes in computer science*(pp. 127–142). https://doi.org/10.1007/978-3-030-55196-4_8

Arigbabu, A. T., Olaniyi, O. O., Adigwe, C. S., Adebiyi, O. O., and Ajayi, S. A. (2024). Data governance in AI - enabled healthcare systems: a case of the project Nightingale. *Asian Journal of Research in Computer Science*, *17*(5), 85–107. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4752897

Billanes, J., and Enevoldsen, P. (2021) A critical analysis of ten influential factors to energy technology acceptance and adoption. *Energy Reports*, *7*, 6899–6907. https://www.sciencedirect.com/science/article/pii/S2352484721009240

Brodin, M. (2019) A framework for GDPR compliance for Small- and Medium-Sized Enterprises. *European Journal for Security Research*, *4*(2), 243–264. https://doi.org/10.1007/s41125-019-00042-z

Gobeo, A., Buchanan, W. J., and Fowler, C. (2022) *GDPR and cyber security for business information systems*. https://doi.org/10.1201/9781003338253

Habbal, A., Ali, M. K., and Abuzaraida, M. A. (2024) Artificial Intelligence Trust, risk and security management (AI trism): Frameworks, applications, challenges and future research directions. Expert Systems with Applications. *Expert Systems With Applications*, *240*, 122442. https://www.sciencedirect.com/science/article/abs/pii/S0957417423029445

Jowarder, N. R. A., and Jahan, N. S. (2024) Quantum computing in cyber security: Emerging threats, mitigation strategies, and future implications for data protection. *World Journal of Advanced Engineering Technology and Sciences*, *13*(1), 330–339. https://doi.org/10.30574/wjaets.2024.13.1.0421

Maroufkhani, P., Ismail, W. K. W., andGhobakhloo, M. (2020) Big data analytics adoption model for small and medium enterprises. *Journal of Science and Technology Policy Management*, *11*(4), 483–513. https://doi.org/10.1108/jstpm-02-2020-0018

Olawunmi, P. O. (2020) *GDPR* and *Data Privacy: Impact of Data Protection in Irish Small and Medium-Sized Enterprises (SMEs)* (By S. Khan). https://d1wqtxts1xzle7.cloudfront.net/97214919/385914677-libre.pdf?1673568355=&response-content-disposition=inline%3B+filename%3DGDPR_and_Data_Privacy_Impact_of_Data_Pro.pdf

Putri, G. A., Widagdo, A. K., and Setiawan, D. (2023) Analysis of Financial Technology Acceptance of Peer to Peer lending (P2P lending) using Extended Technology Acceptance Model (TAM). *Journal of Open Innovation: Technology, Market, and Complexity*, *9*(1), 100027. https://www.sciencedirect.com/science/article/pii/S2199853123001294

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., and Palmatier, R. W. (2022) Digital technologies: tensions in privacy and data. *Journal of the Academy of Marketing Science*, *50*(6), 1299–1323. https://doi.org/10.1007/s11747-022-00845-y

Settembre-Blundo, D., González-Sánchez, R., Medina-Salgado, S., and García-Muiña, F. E. (2021) Flexibility and resilience in Corporate decision making: A new Sustainability-Based Risk Management System in uncertain times. *Global Journal of Flexible Systems Management*, *22*(S2), 107–132. https://doi.org/10.1007/s40171-021-00277-7

Silva, P. (2015) Davis' Technology Acceptance Model (TAM) (1989) In *Advances in knowledge acquisition, transfer, and management book series/Advances in knowledge acquisition, transfer and management book series* (pp. 205–219). https://doi.org/10.4018/978-1-4666-8156-9.ch013

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C., and Platts, J. (2022) Cybersecurity, Data Privacy and Blockchain: a review. *SN Computer Science*, *3*(2). https://doi.org/10.1007/s42979-022-01020-4

Appendix: Survey Questionnaire