VPN SOLUTIONS: BALANCING PRODUCTIVITY AND SECURITY FOR BUSINESS

by

Dr Reji Kurien Thomas, DSc, Fellow in CSR, PhD, M.Tech, MBA

DISSERTATION

Presented to the Swiss School of Business and Management Geneva

In Partial Fulfilment

Of the Requirements

For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

May 2023

VPN SOLUTIONS: BALANCING PRODUCTIVITY AND SECURITY FOR BUSINESS

by

Dr Reji Kurien Thomas

APPROVED BY

Dr. Iva Buljubašić, Ph.D., Chair

Dejan Curović
200016477

Digitally signed by Dejan Curović
200016477
Date: 2023.05.15 21:11:29 +02'00'

Dr. Dejan Curović, Ph.D., member and mentor

Dr. Saša Petar, Ph.D., Committee Member

RECEIVED/APPROVED BY:

SSBM Representative

ABSTRACT

VPN SOLUTIONS: BALANCING PRODUCTIVITY AND SECURITY FOR BUSINESS

Dr Reji Kurien Thomas
2023

Dissertation Chair: <Chair’s Name>
Co-Chair: <If applicable. Co-Chair’s Name>

The COVID-19 pandemic resulted an increase in teleworking to ensure that businesses and employees could continue to function. Teleworking has been acknowledged to have both advantages and challenges. Nevertheless, its success in supporting continuity of business operations has resulted in organisations continuing to support it, in full-time or hybrid modes, even after the pandemic. Relatedly, different technologies have been used to support telework. In this thesis, the impact of using virtual private networks (VPNs) to support productivity and security while organisations continue to allow their employees to telework is studied. The outcomes of this study can help organisations finetune models of work which include teleworking. Moreover, the insights may help organisations redesign work and schedules for different levels of employees.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I:
INTRODUCTION

1.1 Background

The sudden and extended lockdown periods of the Covid-19 global pandemic caused many disruptions to daily existence. One of the immediate impacts was to workers as this resulted in teleworking, that is, “work-from-home” or “home-office,” being recommended and hence implemented by many governments and employers. The other impact was to organisations as they had to revisit the way they operated to ensure that production could be sustained during the pandemic. Indeed, for many industrial sectors, organisations, and employees, this became a comprehensive “forced experiment” where they continued to function despite a state of physical disconnection. Of course, this was only if they had the requisite provisions of ‘technological’, ‘legal,’ and ‘digital security’ (OECD, 2020).

Correspondingly, organisations provided various technological equipment to support teleworking adoption during the Covid-19 pandemic such as, PCs, virtual private networks (VPNs), or similar systems for sharing the organisational network online, platforms to operate virtual meetings, smartphone/company sim card, and business chats (Tokarchuk, Gabriele and Neglia, 2021). It could be seen that VPN, in particular, is regarded as one of the tools to safeguard an internet connection and offset threats of cybercrime (Alashi and Aldahawi, 2020). VPN utilises the concept of tunnelling to establish a secure channel of communication between a device used for teleworking and a remote access server. In this, cryptography is utilised to safeguard the privacy and reliability of the communications (Scarfone, Greene and Souppaya, 2020).

On the whole, while teleworking served to ensure the safety of employees together with maintaining their productivity, it did not necessarily consider the implications as regards cybersecurity on either businesses and employees or the necessity to adequately establish the secure environment required for secure teleworking. Accompanying this is a general perception that home-based information technology (IT) devices are inadequately configured in comparison with IT devices in the workplace. That is, home-based devices have a greater proneness to cyberattacks. Correspondingly, there is the risk that hackers or cyber criminals may prey on unsecured or badly configured routers, modems, and network devices, which are located outside organisational or institutional sites, to take advantage of the weaknesses related to teleworking and thus jeopardizing the security of firms (Abukari and Bankas, 2020). Relatedly, Loia and Adinolfi (2021) highlighted that digital and cyber security are among the negative aspects of teleworking. They acknowledged that the use of ICT (information and communication technology) devices at homes are typically associated with poor configuration and high proneness to cyberattacks (Loia and Adinolfi, 2021).

Teleworking

Teleworking has been described as "the performance of work activities, at a distant location from employing/contracting organisations that is enabled by information and telecommunication technologies" (Kerrin and Hone, 2001, p. 130). In the Covid-19 scenario, this often referred to home-based teleworking. The International Labour Organisation (ILO) notes that this necessitates employers and employees to share a mutual commitment and responsibility to confirm continuity of business and work (ILO, 2020a).

Teleworking, even before the pandemic, had found wide acceptance across different domains such as, knowledge-intensive business services and information and communication services, in the European Union (EU). During the pandemic, teleworking continued to be an optimal solution in these domains with public and private organisations implementing it in the fields of education, public administration, and financial services (Mılası, González-Vázquez and Fernández-Macías, 2021; Nemteanu, Dabija and Stanca, 2021).

Teleworking, even from its origins, has been considered to be an advantageous arrangement for work. Its advantages include enhanced work autonomy which can lead to satisfied employees; and improved performance. In the context of teleworking, work autonomy signifies independence in completing tasks and flexibility in apportioning time for work. Relatedly, the enhancement in autonomy increases the time employees can spend with their families resulting in improved work-life balance (Shardeshmukh, Sharma and Golden, 2012; de Vries, Tummers and Bekkers, 2019; Delanoeije and Verbruggen, 2019, 2020; Dima *et al.*, 2019; Golden and Gajendran, 2019).

Teleworking, however, also has its accompanying disadvantages. For instance, the interaction with colleagues and managers is reduced to the lack of physical proximity. In addition, extended periods of teleworking may result in adverse impacts to individuals including, professional isolation, increased pressure to complete tasks from family or managers, conflict in relations between family and work, and enhanced stress. These individual impacts are often reflected in outcomes related to work and indirectly in the performance of employees; and also, in commitment to the organisation and intent to resign (Shardeshmukh, Sharma and Golden, 2012; Song and Gao, 2018; Golden and Gajendran, 2019; Delanoeije and Verbruggen, 2020).

A study during the pandemic by Green, Tappin and Bentley (2020) highlighted some of the challenges of teleworking such as, social isolation, conflict between home and work, intensification of work, impacts to physical and mental wellbeing, and work performance (Figure 1.1).

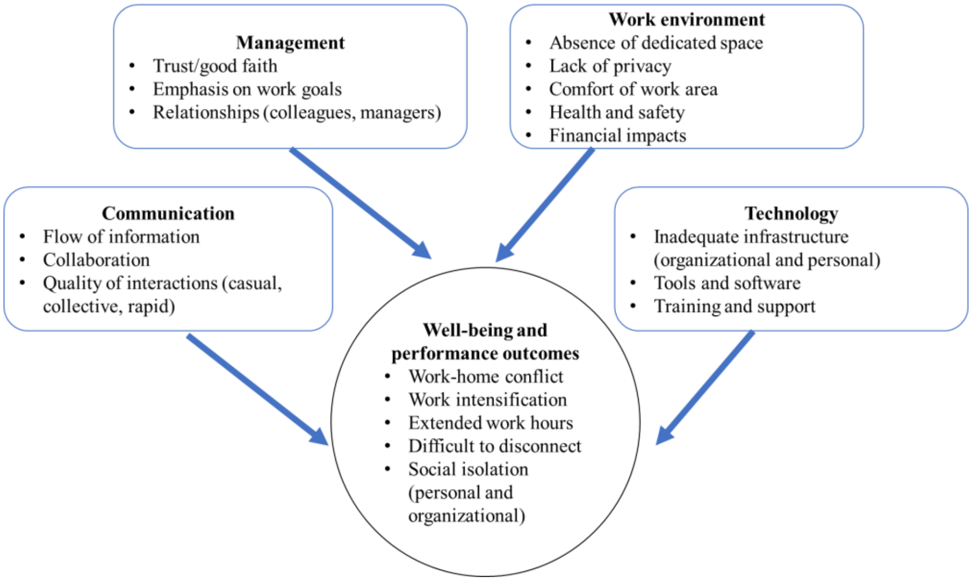

Figure 1.1
Challenges of Teleworking (Green, Tappin and Bentley, 2020, p. 8)

Relatedly, another study by Greer and Payne (2014) highlighted some of the desirable facets of telework such as, flexibility of work, lowering of traffic woes, and decrease of air pollution due to lower traffic. In addition, organisations can attract and retain a diverse workforce and top talent by supporting telework as an alternate work arrangement. In addition, organisations can access a pool of talent outside their geographic location by allowing full-time teleworking. Moreover, teleworking is associated with higher productivity, lower rates of absenteeism, reduced rates of turnover, higher commitment to the organisation, reduced costs of overhead due to the maintenance of fewer number of offices, lower costs of utilities, and reduced costs of real estate, and enhanced performance of the organisation. In addition, teleworking can help organizations increase their conformity to specific governmental regulations and also accommodate persons with disabilities while facilitating business continuity during normal hours of business (Greer and Payne, 2014).

Teleworking Standards

On the whole, while teleworking served to ensure the safety of employees together with maintaining their productivity, it did not necessarily consider the implications as regards cybersecurity on either businesses and employees or the necessity to adequately establish the secure environment required for secure teleworking. Accompanying this is a general perception that home-based information technology (IT) devices are inadequately configured in comparison with IT devices in the workplace. That is, home-based devices have a greater proneness to cyberattacks. Correspondingly, there is the risk that hackers or cyber criminals may prey on unsecured or badly configured routers, modems, and network devices, which are located outside organisational or institutional sites, to take advantage of the weaknesses related to teleworking and thus jeopardizing the security of firms (Abukari and Bankas, 2020). Relatedly, Loia and Adinolfi (2021) highlighted that digital and cyber security are among the negative aspects of teleworking. They acknowledged that the use of ICT (information and communication technology) devices at homes are typically associated with poor configuration and high proneness to cyberattacks (Loia and Adinolfi, 2021).

While technology supported and sustained teleworking, it also introduced greater potential for cyberattacks and breaches of confidentiality (ILO, 2020a). Increasing awareness of these potential dangers, the Information Technology Laboratory (ITL) issued a bulletin in March 2020 which reaffirmed the teleworking standards issued by the National Institute of Standards and Technology (NIST) (Scarfone, Greene and Souppaya, 2020). These standards encompass the following security measures as regards teleworking:

- Forming and applying a policy for telework security, such as, devising various tiers of remote access

- Necessitating enterprise access through multi-feature authentication
- Employing validated encryption technologies to safeguard data and communications archived on client devices
- Making sure that remote access servers are effectively secured and kept up-to-date with the latest security patches
- Protecting all kinds of client devices used for teleworking, such as, desktops, laptops, tablets, and smartphones, against customary threats (Scarfone, Greene and Souppaya, 2020)

Moreover, ITL concurred that teleworking and usage of remote access technologies necessitate further protection as their exposure to external threats is greater in contrast to onsite IT infrastructure (Abukari and Bankas, 2020). Salient IT security concerns and challenges as regards teleworking include the absence of physical security controls as telework can be performed from various locations such as, homes of employees and coffee shops. In addition, the usage of unsecured networks for remote access signifies that organisations typically cannot control the security of the networks utilised by teleworkers. Moreover, organisations encounter new threats since there is a need to allow sensitive resources to be accessed from outside the organisation (Scarfone, Greene and Souppaya, 2020).

In response, organisations were advised to develop security policies and controls for telework on the basis that hostile threats are a feature of external environments (Scarfone, Greene and Souppaya, 2020). Relatedly, it has been suggested that employers needed to take measures to ensure maintenance of data security. This could involve ensuring the robustness of their information technology system with required safeguards, such as, the secure transmission of sensitive data, and ensuring that work computers have appropriate software, such as, anti-virus protection, safe virtual private networks (VPNs, or firewalls against cyber threats (ILO, 2020a).

Efficiency and productivity in teleworking

Regarding productivity in teleworking, research has explored the impact of the social and physical settings at home and future teleworking inclinations (FTI) on employees' productivity (Weber *et al.*, 2022). In addition, there are concerns regarding measuring the productivity of teleworking employees (ILO, 2020a).There has also been mention of the impact of telework on workers' productivity and hence policies related to increasing its economic gains (OECD, 2020). The OECD report in particular notes that "While more widespread telework in the longer-run has the potential to improve productivity and a range of other economic and social indicators (worker well-being, gender equality, regional inequalities, housing, emissions), its overall impact is ambiguous and carries risks especially for innovation and worker satisfaction" (OECD, 2020, p. 2). Additionally, researchers such as Sanhokwe and colleagues (2022) found that the employee teleworking experience was influenced by their perceived workload and the support they received from the organisation. Moreover, their productivity was influenced by their engagement with work. Moreover, teleworking has been reported to help employees improve their productivity as they escape from inconsequential duties while also reducing their time taken to commute to work (Kazekami, 2020).

Relatedly, the Model of Teleworking (Baruch and Nicholson, 1997) and the Crisis-induced Telework Adjustment framework (Carillo *et al.*, 2021) highlight that typically four simultaneously-present factors impact the effectiveness of telework. These include job factors that signify the character of work and the technology utilised for certain work-roles; organizational factors that indicate the extent to which the organisation supports telework, including facets such as the trust exhibited by managers towards teleworkers; home/work factors such as, good physical settings, quality of family relations, and available facilities; and individual factors or personal characteristics such as attitudes, personality traits, and needs. In the Covid-specific context, Carillo and colleagues (2021) highlight that certain unique aspects should be considered as regards teleworking during COVID-19 such as, stress due to the pandemic-related uncertainty concerning health and occupation; restricted access, due to school closure and shutting down of facilities for child-care, to child-care support; societal and professional separation; and conflict between family- and work-requirements.

In a quantitative study, Mihalca, Irimias and Brendea (2021) examined the relationship between individual, job, home/family, and organizational factors and becoming accustomed to telework during the pandemic. Using Baruch and Nicholson's Model of Teleworking, this study obtained data from 482 employees who were full-time teleworkers. The findings of the study indicate that performance, productivity, and satisfaction of employees while teleworking are impacted by individual aspects (e.g., self-management strategies) and aspects of home/family (e.g., the necessity for sufficient telework conditions). In addition, job facets (e.g., workload) also served to impact employees' productivity and satisfaction.

Teleworking has also been associated with increased stress and detriments to productivity over extended periods of time in comparison with in-office levels in some contexts, such as public organisations (Drumea, 2020). This study found that work productivity was negatively influenced by factors such as, disturbed work/life balance, challenges with online communication, and enhanced anxiety. The disturbances to work/life balance were due to the increased number of hours spent working every day, unclear lines between hours of work and leisure hours, modified work routine and related frustration. Challenges with online communication included concerns with IT, connectivity in general, or internet or network, in particular. The enhanced anxiety was related to loneliness, restriction, post-COVID-19 situation, or the need for new competencies to telework. In contrast, positive influences on work productivity were enhanced work/life balance, advantages of online communication, and lowered anxiety. Enhanced work/life balance was attributed to more effective planning and usage of working hours due to flexibility of schedule, time gained due to non-commuting, modified working routine and related comfort. Advantages of online communication included enhanced flexibility in discussion with lower formality and communication on "own terms". Lowered anxiety was due to lower exposure to contamination in the COVID-19 scenario and new opportunities, in general, and the opportunity to learn/develop new competencies, in particular (Drumea, 2020).

Alotaibi and Alharbi (2022) used sentiment analysis to investigate the perception of users in Saudi Arabia toward teleworking. Their analysis of tweets with hashtags referring to the teleworking program in the country indicated that the majority of the users had neutral sentiments towards teleworking followed by persons with a positive sentiment. Overall, flexibility, team work, preference for teleworking, and learning were the significant themes associated with positive feelings towards teleworking. On the other hand, negative sentiments were related to the private sector, organisations, and fake job opportunities offering teleworking (Alotaibi and Alharbi, 2022).

A study by Ionescu and colleagues (2022) explored the implementation of telework in Romania during the pandemic. The findings of this study revealed that the majority of the participating employees (81.10%) preferred a return to office. On the other hand, 7.8% of participating firms wanted to sustain the implemented telework conditions whereas 12.30% wanted to develop their practices to support telework. A further 27.60% were satisfied with their current implementation of telework methods.

Instruments used by the firms for telework included computer/laptop, phone, and tablet. Methods used for telework included email, phone calls, and online conferences (Ionescu *et al.*, 2022).

An OECD report discussed the findings of a survey conducted by the Global Forum on Productivity (GFP). This survey involved managers and employees from 25 countries and was associated with their experiences and expectations as regards teleworking. Overall, teleworking was perceived favourably from the perspective of both firm performance and the well-being of individuals (Criscuolo *et al.*, 2022). A further finding that in the current post-COVID19 context, respondents considered that teleworking for 2-3 days per week was ideal. The study found that organisations' experience with telework differed by their size. In addition, the findings supported other research that found that there was a need to balance the benefits and costs of teleworking in a hybrid working mode (Criscuolo *et al.*, 2022).

Technological Support for Teleworking: Virtual Private Networks (VPN)

Binkhorst and colleagues (2022) described VPN as a "cornerstone of security advice" for users of the Internet. This, perhaps, is due to their usage in countering censorship, filtering geographical content, surveillance at the state-level, invasions of corporate privacy, and threats of unsecured local access to the Internet (Nobori and Shinjo, 2014; Wang *et al.*, 2017; Khan *et al.*, 2018; McDonald *et al.*, 2018; Molina, Shyam Sundar and Gambino, 2019).

A study by Binkhorst and colleagues (2022) explored the contrast in the usage of corporate and public VPNs. Corporate VPNs signify the usage of VPNs in a corporate context to "manage and connect remote workstations to internal corporate resources" (Binkhorst *et al.*, 2022, p. 1). Binkhorst and colleagues (2022) reported that connection to the VPN was perceived to be a part of the daily process of teleworking. Moreover, VPN was perceived to mitigate threats such as, external parties listening in on communication and stopping malicious software, but also introduce new ones such as, lowered reliability, enabling unauthorised access, and privacy issues. In addition, different groups of users (e.g., experts and non-experts) were found to have different perspectives regarding the knowledge of VPN infrastructure and threat management through they were aligned as regards the fundamentals of VPN usage. Figure 1.2 depicts the perceptions of experts and non-experts as regards the usage of VPN.

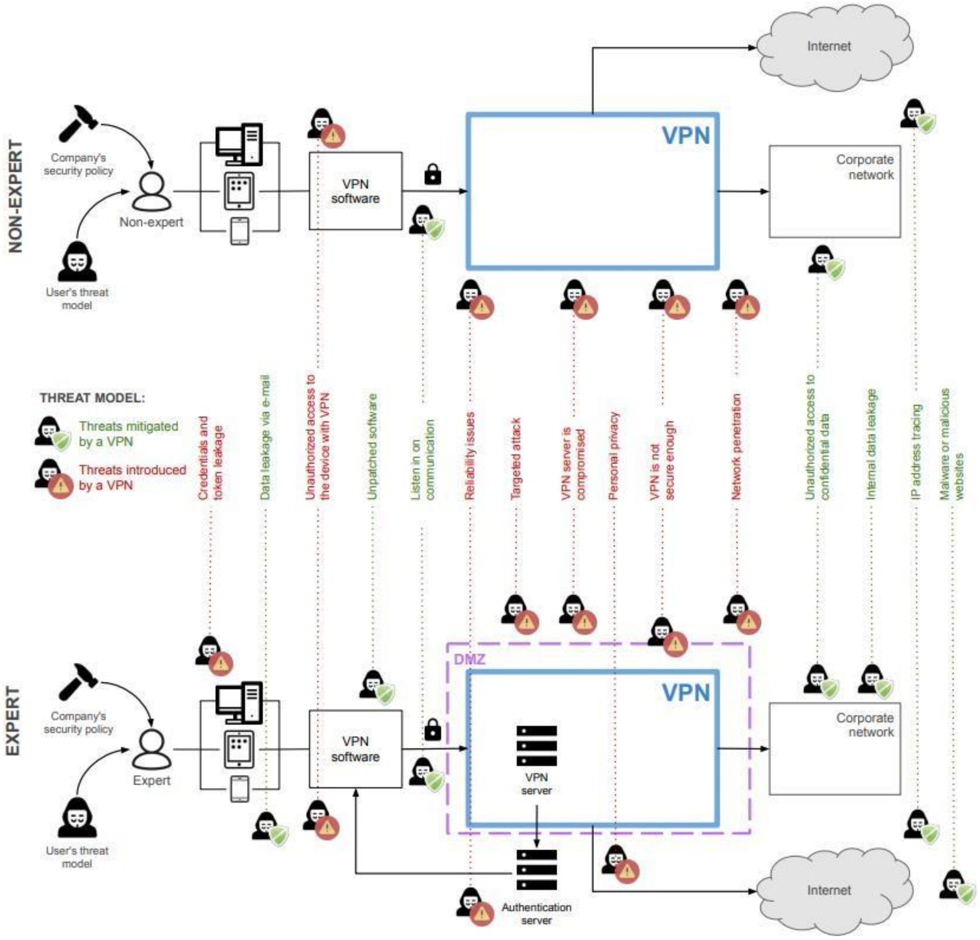

Figure 1.2:
Mental Models for VPNs

(Binkhorst *et al.*, 2022, p. 10)

In another study, Turner and colleagues (2020) concluded that while employees trusted the cyber security protocols (e.g., VPNs and platforms for teleworking) implemented by their organisations during the pandemic, they were not as confident as regards the efficiency and performance of these protocols in contrast to the in-person working scenario.

Other studies have focused on the technical aspects of using VPN in teleworking environments. For example, de la Cruz and colleagues (2020) described the OpenVProxy teleworking environment which is intended to be implemented in various computer network environments. This study highlighted the contribution of OpenVPN encrypted tunnels as regards secure teleworking, in particular, as regards compliance to requirements of confidentiality, integrity, and availability (CIA). Further, de la Cruz and colleagues (2020) indicated that VPNs offer a means for remote networks to communicate in a secure and encrypted manner using a tunnelling approach. Chávez (2020), on the other hand, highlighted how protocols such as PPTP/MPPE (Microsoft Point to Point Encryption), are utilised in VPN to support 40/128 bit encryption.

Another study (Bucșă, 2020) highlighted three teleworking situations where VPN can be of use: usage of employer-provided equipment for data processing, usage of an employee's own system, and the usage of cloud technology. In the latter two situations, the employer lacks control over the security of the systems used by the employees. Consequently, there is a need to establish working guidelines and processes to safeguard the safety and reliability of the data remotely accessed/processed by employees. The usage of VPN ensures that data transmitted over the Internet are encrypted, at least at a low level, through the different stages of transmission. The data are decrypted after their arrival at the destination system. Consequently, Bucșă (2020) recommended that teleworking employees must use a VPN solution compatible with their employer's requirements to deal with cybersecurity threats such as, data leakage. However, the findings of Powell (2021) highlighted that teleworking employees have the tendency to overlook the security protocols of their employers, enhancing the threat of cyberattacks for organisations which engage in large-scale teleworking.

A further emphasis of present-day research is the connection of cybersecurity protocols with efficiency and productivity in teleworking. In this regard, Turner and colleagues (2020) noted that while teleworking employees trust the cybersecurity protocols such as, VPNs and platforms for teleconferencing, implemented by their organisations, they perceive that these are not as safe or reliable as working arrangements that are more in-person. In this regard, Chávez (2020) suggested the use of VPN and multi-factor authentical (MFA) together with a private internet connection to safeguard organisational data and information during teleworking.

On the other hand, Meneses and colleagues (2020) highlighted that while VPNs facilitate controlled remote access, they do not consider the needs of highly mobile users who traverse different kinds of access networks, while needing to retain access to restricted content on corporate networks. Further, they highlighted the disassociation of VPN mechanisms from mobility procedures, a facet that can result in service disruption or the need for specific clients and mechanisms in the equipment of end-users. They propose a framework which aims to offer the extension of VPN in shared networks Wi-Fi without needing the installation of VPN processes or clients on user equipment.

Korty and colleagues (2021) discussed Indiana University's decision to undertake a tailored, risk-based approach to manage their level of VPN provision and usage. One aspect of this approach entails the need for users to utilise VPN only when access to the service cannot be obtained from outside the university. This offers a layer of augmented authentication for such services. A second aspect pertains to the enabling of split tunnelling to ensure that home-to-cloud and personal traffic does not transit the university’s VPN and network. Considerations taken by the university in this regard include the prospect of fewer protected resources, lower flexibility during crises, and overwhelming costs.

Alashi and Aldahawi (2020) proposed a framework to govern the usage of VPN applications to increase the robustness of cybersecurity management. This study found that free VPN applications comprised a significant proportion of VPN use. Alashi and Aldahawi (2020) highlighted that the use of VPN applications is not completely risk-free. Different kinds of risks that may arise include threats to the security of electronic data and information, operating systems, wireless networks, hardware, and even a country. They therefore highlighted the need for ethical use of VPN which is connected with users’ personal and demographic features. Their framework contains three dimensions namely, legal, organisational, and awareness. The legal dimension pertains to the governance of VPN application usage. The organisational dimension encompasses management of risks associated with VPN applications, and policies and procedures for the use of VPN applications in organisations. Finally, the awareness dimension relates to initiatives as regards increasing awareness of the risks of VPN applications (Figure 1.3).

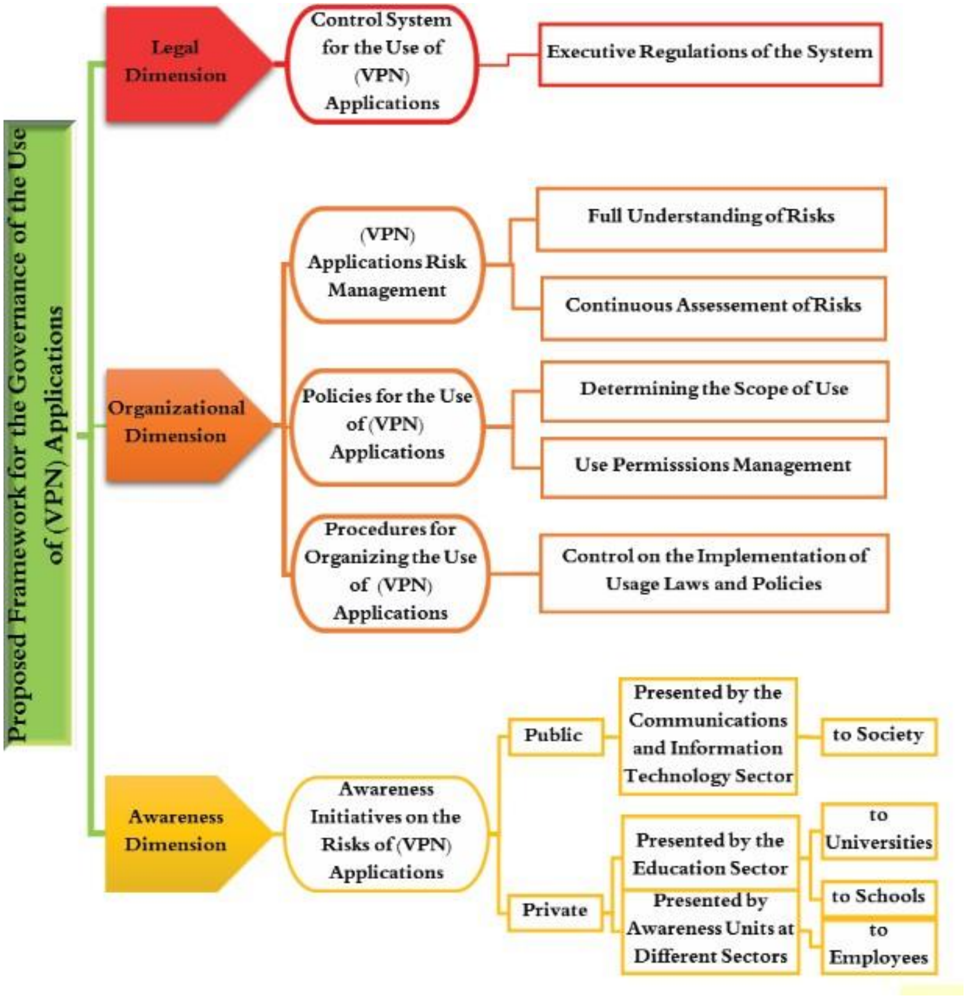
Proposed Framework for the Governance of the Use of (VPN) Applications
Legal Dimension
Control System for the Use of (VPN) Applications
Executive Regulations of the System
Organizational Dimension
(VPN) Applications Risk Management
Full Understanding of Risks
Continuous Assessement of Risks
Policies for the Use of (VPN) Applications
Determining the Scope of Use
Use Permisssions Management
Procedures for Organizing the Use of (VPN) Applications
Control on the Implementation of Usage Laws and Policies
Awareness Dimension
Awareness Initiatives on the Risks of (VPN) Applications
Public
Presented by the Communications and Information Technology Sector
to Society
Private
Presented by the Education Sector
to Universities
to Schools
Presented by Awareness Units at Different Sectors
to Employees

Figure 1.3:
Framework for the governance of VPN use (Alashi and Aldahawi, 2020, p. 54)

1.2 Problem Statement

Organisations have always been interested in improving the productivity of their employees while simultaneously ensuring the security of their data and operations. In this regard, prior research has explored the usage of different technologies to support security and productivity. Teleworking research, in particular, has highlighted the usage of VPNs to support teleworking. In the aftermath of the COVID-19 pandemic there is certainly an increased need for organisations to revisit and re-examine their experience with VPN usage to support extensive teleworking. This will help technologists and practitioners to finetune not only the technological aspects of VPN but also processes and policies to implement VPN in organisations with the intent of balancing productivity and cybersecurity.

For this reason, this study will focus both on the impact of VPN on productivity and security in teleworking, and also the learnings from the experiences of organisations who use VPN to support their teleworking employees.

1.4 Significance of the Study

Overall, the findings of this study are anticipated to help organisations creatively explore opportunities to design different models of work which incorporate teleworking for flexibility while supporting productivity and security. In addition, leaders may receive insights as regards facilitating redesign of work and improving scheduling so as to optimise workloads for different levels of employees. A further implication of this study is the possibility that organizational competencies, on the whole, can be upgraded or enhanced to support the use of different models of work. Additionally, organisations can collect and use productivity- and security-related data to continuously evolve and finetune teleworking policies and processes.

1.5 Research Purpose and Questions

The long-term objectives of the present study are to offer insights regarding the role of VPN in supporting productivity and security while employees continue to use the option of teleworking in the post-COVID scenario. That is, to identify the facets that may contribute to productivity and cybersecurity through VPN usage in organisations.

The objectives of the research can be summarised as follows:

1. To investigate the support provided by VPN usage to achieve productivity and security in the teleworking scenario in the post-COVID context

2. To determine the features of the usage of VPN by organisations to support teleworking employees
3. To gain insights regarding the risks and benefits of VPN usage in this context
4. To identify the facets of a conceptual framework to promote productivity and cybersecurity through VPN usage in organisations which support teleworking

The following overarching research question is used to inform the study:

- Can productivity and security be achieved in the teleworking scenario in the post-COVID context through the usage of VPN?

The associated sub-questions are also proposed:

1. What are the features of the usage of VPN by organisations to support teleworking employees? That is, how is VPN used by organisations to support teleworking employees?
2. What are the risks and benefits of VPN usage in this context? That is, is the usage of VPN to support teleworking beneficial or risky for organisations?
3. What are the facets of a conceptual framework to promote productivity and cybersecurity through VPN usage in organisations which support teleworking?

1.6 Definitions of key terms

The study uses the following understanding of the keywords and phrases:

- *Telework:* “the work performed through the use of information communication technology (ICT’s such as smartphones, tablets, laptops and desktop computers) outside the employer’s premises” (ILO, 2020b, p. 6)

- *Teleworking:* “the performance of work activities, at a distant location from employing/contracting organisations that is enabled by information and telecommunication technologies” (Kerrin and Hone, 2001, p. 130).
- *Employee Productivity:* “the efficiency and effectiveness of individuals in completing tasks and work responsibilities” (Afrianty, Artatanaya and Burgess, 2022, p. 51)
- *Effectiveness:* “extent to which an employee can complete their responsibilities in accordance with a predetermined deadline” (Afrianty, Artatanaya and Burgess, 2022, p. 51)
- *Efficiency*: “the extent to which the individual can accomplish tasks and responsibilities without any *waste* of resources” (Afrianty, Artatanaya and Burgess, 2022, p. 51)
- *Virtual private networks (VPN)*: “an *encrypted* connection over the Internet from a device to a network” (CISCO, 2022).

1.7 Thesis organisation

The progress of this research to achieve the objectives of the study and answer the research questions is organised into six chapters (Figure 1.4). The first chapter, **Chapter 1 (Introduction),** provides the background for the study and introduced the perspectives of teleworking, teleworking standards, efficiency and productivity in teleworking, and technological support for teleworking. Moreover, it described the problem statement, identified the research question and objectives of the study, and highlighted the significance of the study. In addition, the key terms utilised in the study were introduced.

The second chapter, **Chapter 2 (Review of Literature)** offers a review of past literature associated with the theme of the current study such as, teleworking, productivity in teleworking, security and teleworking, VPN, and technology support for teleworking. The preliminary visualisation of the proposed conceptual framework will also be provided.

In the third chapter, **Chapter 3 (Methodology)**, the methodology adopted to achieve the objectives of the study will be described. Since the researcher believed that the case study approach would be most appropriate in investigating productivity and security in the current post-COVID work context. Hence the chapter will describe the case study approach along with the research design, instruments and processes adopted for this study. This will include methods for collection and analysis of data, and techniques for sampling.

The fourth chapter, **Chapter 4 (Results)**, will present the findings of the study from the data obtained from the case study. **Chapter 5 (Discussion)** discusses the findings of the study in the light of existing literature and answers the research questions. In addition, the final visualisation of the proposed conceptual framework will be provided. The final chapter, **Chapter 6 (Conclusion)**, will provide a summary of the study and its findings. In addition, the conclusions and implications derived from the findings will be highlighted. Recommendations will also be made based on the findings. Suggestions will also be provided for future researchers.

Introduction
Review of Literature
Methodology
Results
Discussion
Conclusion

Figure 1.4:
Thesis organisation

CHAPTER II:
REVIEW OF LITERATURE

2.1 Chapter Introduction

As highlighted in the Introduction to this thesis, the overarching objective of this study is to offer insights regarding the role of VPN in supporting productivity and security while employees continue to use the option of teleworking in the post-COVID scenario. Consequently, a review of the current research in the area is provided to highlight the need for the present study. Accordingly, this chapter will review recent research related to telework and teleworking, the types of telework arrangements, job characteristics in teleworking, and factors that influence telework. In addition, research related to the impacts of teleworking on employee well-being, efficiency and productivity, and security will be reviewed. Furthermore, this chapter will include research on VPNs and the role of technology to support teleworking. The chapter will conclude by summarising the perceived research gap and by providing the preliminary conceptual framework for productivity and cybersecurity through VPN usage in the continued use of teleworking in organisations based on the review of literature.

2.2 Telework and Teleworking

Telework, also referred to as remote work, has been defined as “is a form of organising and/or performing work, using information technology, in the context of an employment contract/relationship, where work, which could also be performed at the employers pre- mises, is carried out away from those premises on a regular basis” (European Trade Union Confederation *et al.*, 2002, p. 2). Relatedly, any person performing telework is a teleworker. Telework is considered to be an intentional decision both for the worker and the concerned employer. Consequently, the need for teleworking may be an element of the preliminary job description of a worker or may be taken on as a deliberate understanding. Accordingly, the teleworker is provided with applicable written information by the employer, in either instance, compliant with related directives. This information typically includes information on related mutual contracts, specification of the work to be undertaken, etc. The particulars of telework generally necessitate supplementary recorded information on subjects including the teleworker's department in the firm, his/her direct superior or other individuals to whom queries of individual or professional character, reporting arrangements, etc., can be addressed (European Trade Union Confederation *et al.*, 2002).

According to the ILO, telework presents "a modernization of the organization of work, aimed at increasing undertakings productivity and competitiveness, whilst achieving the necessary balance between business flexibility requirements and workers' security aspirations, enhancing job quality and promoting the access to formal labour market to particularly vulnerable groups of workers (e.g., workers with family responsibilities, workers with disabilities, etc.)" (ILO, 2020b, p. 8). Telework has some advantages for both firms and employees. First, it is viewed as an approach to streamline organisation of work by establishing work arrangements that are flexible and more independent. Second, it facilitates achievement of improved resolution of professional, individual, and family life. Moreover, telework helps lower carbon emissions from traveling to work and hence has a favourable effect on the environment. In addition, it is also viewed as an essential component to achieve goals regarding jobs and development with specific regard to labour market modernization and the advancement of the information society in an economy which is knowledge based (ILO, 2020b).

A study set in Chile by Astroza *et al.* (2020) about teleworking during the pandemic found that income was a significant determinant of employees who were eligible to telework. That is, while high-income workers could telework, low-income workers had to continue to go out to the workplace. In addition, telework was more likely to be undertaken by women.

Definitions of telework and teleworking

Teleworking, since its inception, has been defined in different ways. For example, Baruch and Nicholson (1997, p. 16) define it as "An employee who performs all or the greater part of their work from a domiciliary base, physically separate from the location of their employer." Olson (1983, p. 182) referred to it as remote work and defined it as "organizational work performed outside of the normal organisational confines of space and time."

Beckel and Fisher (2022, p. 1) defined telework as "working outside of the conventional office setting, such as within one's home or in a remote office location, often using a form of information communication technology to communicate with others (supervisors, coworkers, subordinates, customers, etc.) and to perform work tasks."

Belzunegui-Eraso and Erro-Garcés (2020, p. 2) described telework as a form "of work and/or provision of services done remotely, at a distance, and online using computer and telematics technologies." In other words, it refers to work accomplished through the aid of ICTs and performed external to the locations of the firm.

Burton *et al.* (2021) highlighted the multitude of definitions and approaches related to teleworking. Drawing on previous researchers (e.g., Daniels, Lamond and Standen, 2001; Hyman and Summers, 2004; Morganson *et al.*, 2010; Pyöriä, 2011; Mahler, 2012), they noted that even in among organisations, teleworking arrangements are not always comparable and are not always compatible or appropriate for every employee. Moreover, even employees in the same role in the same firm may not have comparable views of teleworking. Consequently, Burton *et al.* (2021, p. 3) defined teleworking or telecommuting, derived from different researchers (Stern and Holti, 1986;

Andriessen, 1991; Fitzer, 1997; Garrett and Danziger, 2007), as “working away from the employers’ main campus (including working in a satellite office, home-based working, or mobile working) whilst supported by various technological solutions.” They also summarised the different understandings and definitions of teleworking obtained in literature (Table 2.1).

Table 2.1:
Definitions of teleworking (Burton *et al.*, 2021, p. 4)

Definition	**Description**	**Advantages**	**Disadvantages**
Home-based teleworking	Duties performed in the home of an employee	Lessening in work/life conflict; Lowered time for commuting; can enhance satisfaction with job; provides flexible working agreements [with option to work from home] can increase the attractiveness of jobs for applicants.	Feeling of separation from teams; possible ambiguity of role, enhanced inclination to be concerned and anxious; possible surge in hours of working; expense of developing facilities for home office.
Satellite or client-based teleworking	Duties performed away from the main campus of the employer but still in a premises controlled by employer or a client	Frequently a function of needs of the firm and/or lower time to commute	No intrinsic use for work/life balance; employees can get the impression they are on the organisation’s fringes; and separation from authority.
Mobile teleworking	Duties are performed from no permanent site, frequently aided by mobile devices, for instance, repairs or field sales	Fundamental to the performance of a role in some instances; elevated extent of independence	Dependence on availability of network; Is dependent on considerable self-will. Does not support work/life balance

Types of Telework arrangements

Telework arrangements can be either for a temporary period or of a more long-standing duration. Short-term telework arrangements are ad-hoc or scheduled remote work arrangements while long-term arrangements are termed fixed remote work agreements (ILO, 2020b). Ad-hoc remote work signifies situations where an employee needs to be away for some hours or for a day from the employer site. This is typically aimed at dealing with an immediate issue such as, an issue at home or to address a certain work issue away from likely disturbances in the office. This kind of telework arrangement may stretch out over an extended duration but the plan of the employee and/or employer is to return to the place of work at the earliest. On the other hand, scheduled remote work can be viewed as an arrangement for remote work between an employee and employer which may encompass a combination of work at the firm location and at home or somewhere else. In this instance, the employer and employee might decide to plan some days a week where the work is undertaken at the firm location and some days at the employee's home or someplace else. Lastly, the fixed remote work arrangement is typically agreed upon for a longer time period. In this, the employee works completely away from the firm location (ILO, 2020b).

In 2003, the Statistical Indicators Benchmarking the Information Society (SIBIS) defined four distinctive modes: "telework from home, mobile telework, freelance telework in SOHOs (small office/home office), and telework done in shared facilities outside of organizations and the home" (Belzunegui-Eraso and Erro-Garcés, 2020, p. 2). Indeed, through telework, workers are allowed to work from their residences, from common resources, at customer locations, or through any platform with the needed technologies. Hence, it can be concluded that the resources utilised (technology) and the site ascertain the measurement and the idea of telework. Moreover, the mode of telework contemplated is also impacted by frequency (Belzunegui-Eraso and Erro-Garcés, 2020).

Table 2.2 summarises different kinds of telework.

Table 2.2:

Different kinds of telework (Belzunegui-Eraso and Erro-Garcés, 2020, p. 3)

Mode	**Technology usage**	**Location**
Regular home-based	Continually or nearly all the time	From home on numerous every month at the minimum And Less often at other locations

High mobile	Continually or nearly all the time	In two locations (not including employers' premises) at the minimum many times in a week Or Working everyday in one other location at the minimum
Occasional	Continually or nearly all the time	More infrequently And/or lesser locations than high teleworking

Job characteristics in teleworking

Olson (1981) suggested there were certain typical features of jobs related to teleworking. These were:

1. A high extent of intellectual, rather than physical work;
2. Work is performed as an individual, or with distinctly defined spheres of individual work;
3. A reasonable extent of creativity, working at employer-provided goals under specifications of least supervision;
4. Output or deliverables that can be measured;
5. Measurable criteria for performance effectiveness;
6. No necessity to manoeuvre items of equipment that are extremely large or expensive.

A later study by Olson (1983) also suggested that there were certain typical features of jobs related to teleworking. These features were comparatively unrelated to the technology used in a job or the level of the job. The features include:

1. Minimum physical requirements: This signifies that there were minimal physical requirements as regards equipment and space. The maximum requirement was for a client device and connectivity in the home.
2. Individual control over pace of work: Work was typically project-oriented with extended dates for completion.

3. Defined deliverables: the output of the job was controlled in terms of deliverables that were well-defined.
4. Need for concentration: all work requires considerable levels of concentration for some amount of time at the minimum.
5. Defined milestones: all work had milestones that were well-defined with interim deadlines that were easy to define or measure.
6. Relatively low requirement for communication: while the level and type of communication needed varies by job, in teleworking the employee can work for comparatively long time periods with no or little communication with the main office.

Belzunegui-Eraso and Erro-Garcés (2020) highlighted that requirements for telework changed during the COVID-19 pandemic (Table 2.3).

Table 2.3:
Change in telework requirements (Belzunegui-Eraso and Erro-Garcés, 2020, p. 13)

Considerations	**Pre-COVID-19**	**During COVID-19**
Voluntary in nature	Yes	No
Individual agreement	Yes	No
Reversibility	Yes	No
Equality of rights between teleworkers and workers at the employers' premises	Yes	Yes
Work equipment facilitation and installation	Yes	Software only
Ergonomic elements	Yes	No
Technical support	Yes	Yes
Costs of telework	If required	If required
Health, social security and job security	Yes	No
Right to union representation	Yes	Yes
In-company training	Yes	Yes
Preservation of economic conditions	Yes	Yes
Modifications in the statute of rights for workers	No	No

Carillo *et al.* (2021) highlighted various differences in typical telework and telework induced by the COVID-19 epidemic (Table 2.4).

Table 2.4:
Comparison of telework features (Carillo *et al.*, 2021, p. 71)

Features	**Regular telework**	**Telework induced by the pandemic**
Characteristics of telework		
Workplace	Flexibility of workplace: at employee residence and/or at a premises other than the established workplace	Compulsory at home due to lockdown
Use of ICT	ICT as a method of connection, association, and interaction with other professionals and the firm A planned method to utilise ICT to reorganise the manner of working	ICT as a method of connection, association, and interaction with other professionals and the firm ICT as a requisite to ensure continuity of the business
Organisation of working hours	Working hours are flexible	Working hours are flexible with potential limitation of availability of co-teleworkers at the same location and time and/or responsibilities at home
Proportion of working time	All or few of the hours of work	Full-time
Telework Environment		
Implementation	Chosen by employee Planning of physical tele environment, access to technology, and ICT tools Planning of processes of telework, methods of working, and supervisory guidelines	Compulsory with no agreement from employee Unexpected without time for preparation and possible absence of teleworking tools Unexpected without time for preparation for teleworkers, supervisors, and firms
Context of work	Reliable infrastructures and access to ICT Reliable health and financial setting	Reliable infrastructures and access to ICT Concerns with health and job insecurity

Factors that influence telework

Various models have been proposed to explain the factors that influence teleworking. One of the early models is the Model of Teleworking (Baruch and Nicholson, 1997) which highlights that teleworking is influenced by four elements or realms. That is, elements pertaining to individual, job, organizational, and family/home (Figure 2.1). Baruch and Nicholson (1997)indicated that the feasibility and effectiveness of telework was dependent on the fulfilment of these elements. It may be noted that at the time of their study, homeworking was not a popular phenomenon. Hence, Baruch and Nicholson (1997, p. 27) concluded that the implication is that “only when *all* four are satisfied, can home working be practised effectively.”

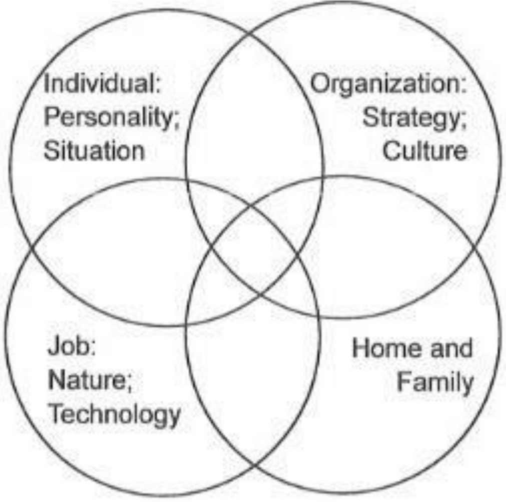

Figure 2.1:
Four elements of teleworking/homeworking (Baruch and Nicholson, 1997, p. 27)

Belzunegui-Eraso and Erro-Garcés (2020) extended the Model of Teleworking to include Environmental, Safety, and Legal factors (Figure 2.2). Environmental factors signify the impact of teleworking on the environment. That is, these are factors related to teleworking’s contribution to reducing pollution and carbon footprint due to reduced travel to the workplace (Ursery, 2003; Irwin, 2004; Manser *et al.*, 2004; van Lier, De Witte and Macharis, 2012). On the other hand, the legal/regulatory factor signifies the absence of specific regulations related to teleworking (Larsen and Andersen, 2007; Prosser, 2011; Pyöriä, 2011). Finally, the safety factor signifies the criticality of telework in safeguarding employees from issues resulting from natural disasters, attacks from terrorists, or health alerts, while ensuring that the organisation can survive by mobilising the workforce while infrastructure and public services are restored (Golden, 2009; Donnelly and Proctor-Thomson, 2015).

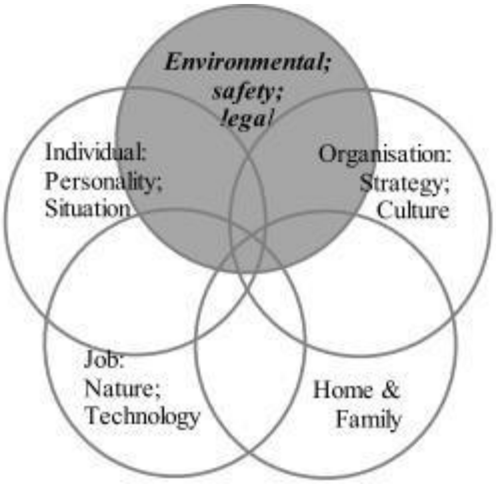
Environmental; safety; legal
Individual: Personality; Situation
Organisation: Strategy; Culture
Job: Nature; Technology
Home & Family

Figure 2.2:
Extended Model of Teleworking (Belzunegui-Eraso and Erro-Garcés, 2020, p. 6)

Beckel and Fisher (2022) derived a conceptual model (Figure 2.3) through a comprehensive literature review related to the antecedents, outcomes, mediators, and moderators of telework at the individual, social, and organizational levels. This model offers a holistic picture of factors associated with telework and health and well-being of workers. The different antecedents include demographics (e.g., gender, age, location, physical environment, occupation, and industry), job characteristics, extent of telework, individual differences (personality, boundary preferences), economic factors (commute time, economic resources), ergonomic resources (training, information and communication technology), and organizational factors (support for telework, formality). Outcomes of telework include health outcomes (physical health, health behaviours, musculoskeletal and pain symptoms, mental health, and psychological well-being), health social and family outcomes (work/family conflict and balance, interpersonal relationships), and work-related outcomes (job satisfaction, absenteeism/presenteeism). Mediators in the model are job characteristics and social context (relationship quality, social support, social isolation) whereas moderators are gender, extent of telework, job characteristics (autonomy, flexibility, task characteristics, voluntariness, boundary preferences).

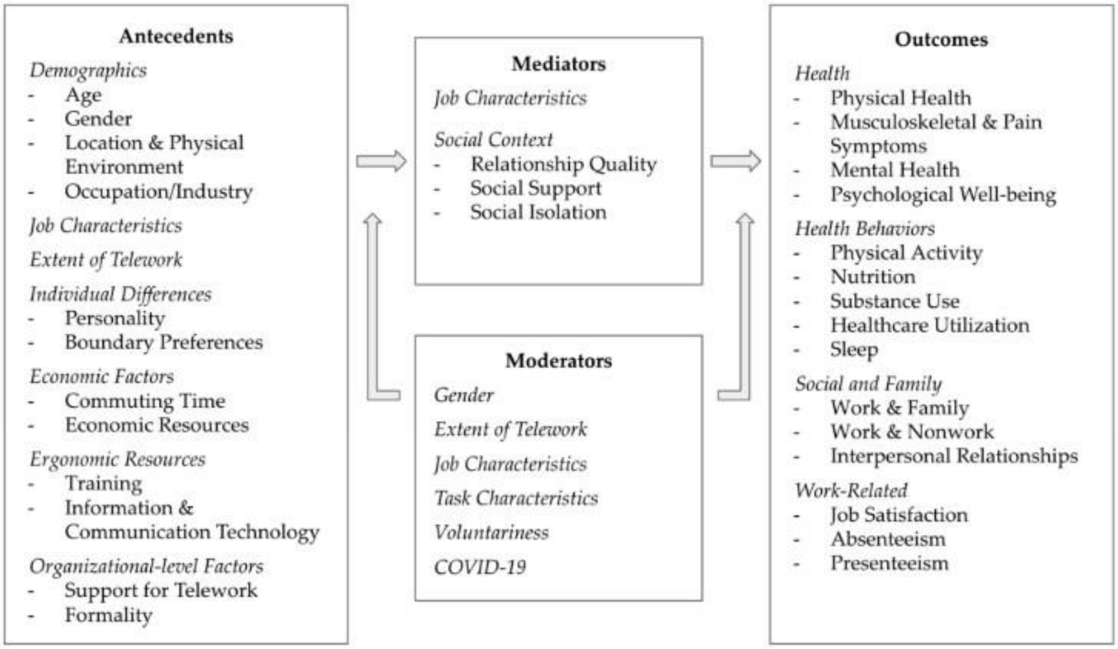

Figure 2.3:
Conceptual model of telework and worker health and well-being (Beckel and Fisher, 2022, p. 5)

Carillo *et al.* (2021) introduced the notion of epidemic-induced telework adjustment and described it as the “employees’ level of adaptation to environmental demands of a new telework context triggered by a global epidemic crisis” (Carillo *et al.*, 2021, p. 73). Using the categories of factors of individual adjustment (Nelson, 1990), this model includes both crisis-specific and non-crisis-specific factors. That is, it includes factors that are influenced or produced by the context of the crisis (e.g., stress, organisational support related to the crisis, or professional isolation), and factors not influenced or produced by the crisis setting (e.g., job autonomy, IT complexity, work interdependence). This model was tested in a study set in France on a sample of 1574 teleworkers and the outcomes indicated that crisis-specific factors are more likely to impact adjustment to telework (Figure 2.4).

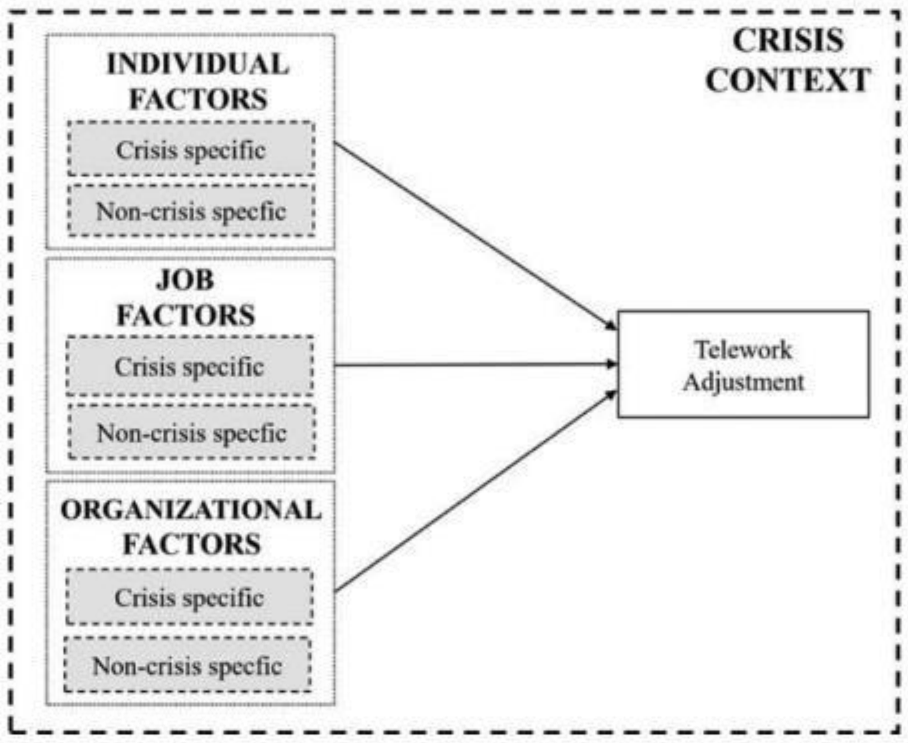

Figure 2.4:
Theoretical framework for Crisis-induced telework adjustment (Carillo *et al.*, 2021, p. 73)

Siha and Monroe (Siha and Monroe, 2006, p. 472; Campbell and McDonald, 2007, p. 814) proposed a model that captured the key factors derived from a review of telework literature. A top-down perspective is followed by this model commencing with a strategic organisational element that is impacted by the setting, regulatory and competitive, in which a firm is functioning. The strategic perspective is moderated by support for telework (from employees and management) and is based on the availability of suitable technologies to support communication. Moreover, impetus is provided in this model for organisations by government regulation and competition to consider strategies for telework (Figure 2.5).

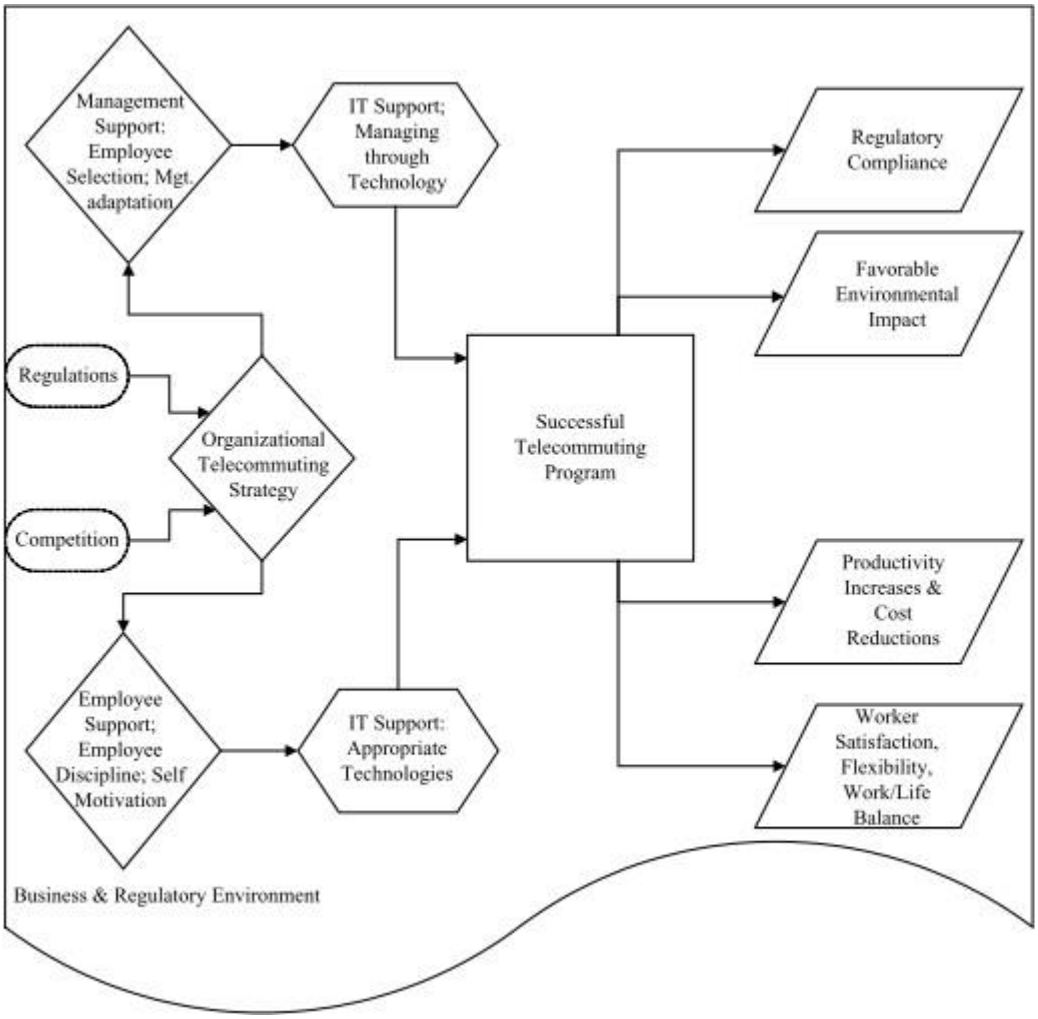
Management Support: Employee Selection; Mgt. adaptation
IT Support; Managing through Technology
Regulatory Compliance
Favorable Environmental Impact
Regulations
Organizational Telecommuting Strategy
Successful Telecommuting Program
Competition
Productivity Increases & Cost Reductions
Employee Support; Employee Discipline; Self Motivation
IT Support: Appropriate Technologies
Worker Satisfaction, Flexibility, Work/Life Balance
Business & Regulatory Environment

Figure 2.5:
Telework/telecommuting success model (Siha and Monroe, 2006, p. 472)

2.3 Impacts of Teleworking

Teleworking has many benefits such as, lowered time to travel and related cost overheads, enhanced independence on the job, flexibility of time, and job satisfaction (Nilles, 1997; Hoeven and van Zoonen, 2015; Camacho and Barrios, 2022). However, teleworking also has various challenges including, work–home conflicts, social isolation, work overload, absence of a feeling of belonging to an organization, and psychological distress (Tietze and Musson, 2004; Kelliher and Anderson, 2010; Chesley, 2014; Kossek, Thompson and Lautsch, 2015). Other impacts of telework include creation of stress, specifically technostress which is related to the inability of teleworkers to deal with fresh ICT requirements in a wholesome manner (Weinert *et al.*, 2014).

Fana *et al.* (2020) attempted to study the impact of telework on job content and dimensions of work organisation such as, team work, schedule, autonomy, and forms and level of supervisory control. They also investigated job quality dimensions including, job satisfaction, changes in working time and pay, motivation, along with issues associated with physical and mental well-being and work-life balance. During the spring lockdown in 2020, the researchers interviewed 75 teleworkers from France, Italy, and Spain. The study found that while teleworkers were positive about their experience with teleworking, they showed a desire to be physically present, at least for some time during the workweek, in the workplace. On the other hand, some of the them believed that their satisfaction and productivity were enhanced when working from home.

Teleworking and employee well-being

Kossek, Lautsch and Eaton (2009) highlighted the psychological facets of job design for teleworking that were associated with favourable outcome for the well-being of employees. Using quantitative and qualitative data from 316 professional employees of two Fortune 500 organisations, this study found that two principal aspects are related to good teleworking. The first is that perceived psychological control over “when, where, and how one teleworks” is significant for well-being. That is, employees experience lesser work–family dispute, intentions to quit, and the likelihood of their wanting to shift to a fresh career is significantly lower when they have better perceptions of their personal control over the place, scheduling, and manner of work. The second aspect influencing employee well-being is related to the manner in which an employee deals with the physical and emotional boundaries between family and work roles. The study found that a strategy for boundary management which supports division of family and work is significantly associated with lesser work–family dispute. Other forms of flexible job design such as, access to formal arrangements for telework, working in various locations, and irregular schedules, are not significantly associated with lesser turnover, preparedness for career movement, or work–family dispute (Kossek, Lautsch and Eaton, 2009).

In another study, Bentley *et al.* (2016) examined the perceptions of 804 teleworkers from 28 organisations in New Zealand where knowledge work was performed in order to determine the role of the organisation in offering social support and particular support for teleworkers in affecting the wellbeing of teleworkers. The study found that enhanced job satisfaction and lowered psychological strain were related to organisational social support and specific support for teleworkers. In addition, the relationship between organisational social support and job satisfaction and psychological strain was mediated by social isolation. Furthermore, the study found some variances in the structural relationships for sub-samples of hybrid teleworkers (telework intensity of >8 hours per week of telework) and low-intensity (telework intensity of 0-8 hours per week of telework) teleworker. Overall, the findings of this study indicating that it was necessary for organisations to provide the required organisational and specific support for teleworkers to enhance the teleworker-environment fit and consequently confirming that the outcomes of telework were advantageous to the organisation (Bentley *et al.*, 2016). Here, teleworker-environment fit signifies teleworking success at the individual level (Haines, St-Onge and Archambault, 2002).

Despite its various advantages, teleworking may also contribute to adverse effects such as, stress. Camacho and Barrios (2022) studied the impact of teleworking on persons who were forced to take it up due to COVID-19 lockdowns in a longitudinal study at two instances (T0, T1) of time. The findings of this study indicate that strain was generated by two “techno-stressors” namely, work-home conflict and overwork. This, in turn, reduced the satisfaction of employees with telework and their perceived performance on the job. Moreover, teleworking employees were found to experience two forms of long-term technostress. The first, synchronous effect, relates to strain-producing stressors at T1, whereas the second, reverse causation effect, relates to the impact on stressors at T1 due to strain at T0.

Productivity in Teleworking

In a recent study, Afrianty, Artatanaya and Burgess (2022) examined the factors that contribute to the productivity of lecturers while teleworking during the COVID-19 pandemic, with specific emphasis on the influence of organisational and individual aspects. The facets considered included digital infrastructure, IT training, and support from management from the organisational perspective, and digital orientation and digital capability from the individual perspective. Using quantitative data obtained from a survey of 267 academic staff from 15 colleges in East Java, Indonesia, this study found that only the digital orientation of an individual had a significant effect on the digital capability of the individual. This, in turn, impacted their productivity while teleworking from home during the pandemic.

Bhattacharya and Mittal (2020) submitted that the individual needs of employees could influence their performance and productivity while teleworking. They highlighted that the boundaries between an individual’s personal existence and office work were getting reduced due to modification in work arrangements. Hence, there was a need to identify the different factors that may influence an employee’s performance. Since home environments (size of family, marital status, Wi-Fi, electricity, reserved laptop with necessary software to telework, noise and other interruptions based on home location, etc.) may differ from person-to-person, the setting for telework also varies and clashes may occur during shifts between work and home, particular when a person's dominant requirements are not fulfilled. Bhattacharya and Mittal (2020) used David McClelland's (McClelland, 1965, 1976) Acquired Needs Theory to categorise these needs into Achievement, Affiliation and Power and studied Home-to-Work conflict (HTWC) and Work-to-Home conflict (WTHC) that may occur in individuals owing to the change in their dominant requirements. Overall, this study found that WTHC and HTWC are impacted by hours spent on work and type of family. In addition, the impact of different dominant requirements is different on conflict outcomes.

Drumea (2020) studied productivity and associated indicators of work performance of teleworkers from public organisations and found that productivity during teleworking was lower than "in-office" efficiency in this context. Factors which negatively influenced productivity included disturbed work/life balance (i.e., the increased hours spent working every day, the indistinct lines between work and non-work hours, modified routine of working and related frustration), challenges of online communication (associated with IT, network connectivity, lower interactions with colleagues), and enhanced anxiety (due to isolation, confinement, need for new capabilities, etc.). In particular, negative productivity was due to IT and network infrastructure and connectivity, and isolation/confinement/worry about the post-COVID-19 scenario. On the other hand, productivity was favourable influenced by the improvement in work/life balance, benefits of online interaction, and lowered anxiety. Specifically, aspects such as gain in time owing to not having to travel to office and lowered anxiety related to exposure in the COVD-19 context were beneficial for productivity.

Golden and Rajendran (2019) investigated the features of teleworkers' work that might aid or obstruct their capacity to undertake their job together with the impact of telecommuting on job performance. Using data from 273 teleworkers and their supervisors, Golden and Rajendran (2019) found that the level of teleworking was positively related to job performance for teleworkers with complex jobs, jobs involving limited degrees of interdependence, and job with lesser degrees of societal support. Further, the findings of this study indicated that the characteristics of a teleworker's work and the extent of teleworking influenced their job outcomes. An earlier study by Golden and Veiga (2005) used a sample of 321 employees and found that there was a curvilinear association between degree of telecommuting and satisfaction with the job. Moreover, facets such as task linkage and job discretion influenced this relationship signifying that some characteristics of the job had a significant, conditional role to play. Additionally, satisfaction seemed to reach a level of stability at greater extents of telecommuting.

2.4 Security and Teleworking

The COVID-19 pandemic highlighted the lack of preparedness of the world to securely deal with working from home. The explosive growth of Internet of Things (IoT) together with the absence of safeguards that are typically available in governmental and organisational premises in employee homes revealed a need for businesses to quickly adapt to the change in situation. The subsequent increase in teleworking as a new standard of work has consequently resulted in the need for the implementation of more robust security (Carnley and Bagui, 2022). In this context, Carnley and Bagui (2022) suggested that 5G, near field communication (NFC), blockchain-based public key infrastructure (PKI), and zero trust architecture securely offer a trusted digital identity for telework.

Mannebäck and Padyab (2021) highlighted four challenges of overarching concern related to teleworking. These are technical security, employee knowledge of security issues, policies and regulations, and, readiness for the novel work setting of teleworking. They summarised the challenges encountered by a case organisation during the pandemic (Table 2.5).

Table 2.5:

Challenges encountered by a case organisation with teleworking employees (Mannebäck and Padyab, 2021, p. 12)

Theme	**Challenge**	**Form of challenge**
Preparedness	VPN that is erratic and un-dimensioned	IT security
Awareness of information security	The levels of employees' knowledge concerning an appropriate set-up for home-office is different	Information security
Technical security	Employees find it difficult to regulate the random character of updates in the home-office setting, i.e., router firmware	IT security
Technical security	Approaches to limit the enlargement of the attack surface	IT security
Preparedness	Worries that employees operate with private devices that are not secure owing to absence of devices owned by the company for employees requiring to telework	IT security
Awareness of information security	Lack of boundaries in the digital space	Information security
Policies and regulations	Absence of instructions regarding the appropriate manner of teleworking	Information security
Awareness of information security	Disproportionate emphasis on IT in comparison with focus on behaviour	Information security
Technical security	Insecure devices used to access email and company internal website	IT security
Technical security	Supervising unauthorised channels of communication	IT security
Awareness of information security	Regulating the environment surrounding the teleworker	Information security
Policies and regulations	Absence of clear rules associated with security of information while teleworking	Information security

The Swedish civil contingencies agency (MSB) offered guidance and teleworking during the lockdown related to teleworking for the organisational teams who coordinate the information security and the teleworking employees. MSB is an agency of the Swedish government that is responsible for matters related to civil protection, safety of public, management of emergencies and civil defence. Organisations were advised to initiate and evaluate their practices for information security associated with teleworking. Questions to be asked included: "What rules apply to teleworking and the use of IT systems outside the organization?" "What capacity does the organization have for how many people can work remotely?" and "Has the organization adopted continuity plans?" (CERT-SE, 2020; MSB, 2020b, 2020a). Furthermore, MSB provided measures for consideration from the perspectives of both organisations and employees (CERT-SE, 2020). Examples for employers include:

- Ensure that employees are familiar with practices and policies related to home work.
- Ensure that employees who telework can access the resources they require to safely perform their job (e.g., two-factor authentication, VPN).
- Ensure adequate staffing of IT support functions due to the increase in the number of queries and support concerning connection from home.
- End users should not be assigned administrator rights.
- Block unauthorized software. Users to be allowed to run only approved applications. (CERT-SE, 2020)

Examples for employees include:

- Do not utilise private equipment for work-related activity unless agreed and approved by employer. Also, usage of private cloud services is to be avoided unless clarified by the employer.

- Ensure that all equipment utilised when teleworking is well up-to-date (e.g., computer hardware, antivirus signatures, operating system, third-party applications).
- Protect all contact with the network and services of the firm, for example, using VPN.
- Ensure sufficient internet capacity and bandwidth
- Ensure that all user accounts have robust passwords, with two-factor authentication if possible.
- Since the risk of endangering sensitive information is greatly enhanced extent when working at home rather than when working in the office, there is a need to be more aware of the kind of information that handled and to ensure that the information can be handled correctly at home as well.
- Disconnect other devices that are not needed for work from the network, such as stream services, to support good internet capacity while working (CERT-SE, 2020)

Teleworkers typically utilise different client devices (e.g., desktops, laptops, smartphones, tablets) to read and send email, visit websites, read and edit documents, and undertake various other activities. These devices may be regulated by the firm, by third parties (e.g., contractors, vendors, business partners of the organisation), or by the users (e.g., bring-your-own device/BYOD). Teleworkers, typically, utilise remote access which can be described as the “ability for an organization’s users to access its non-public computing resources from external locations other than the organization’s facilities” (NIST, 2016, p. 2).

In general, the typical security goals for telework and remote access technologies include: Confidentiality, Integrity, and Availability. Confidentiality signifies ensuring that unauthorised parties cannot access remote access communications and archived user data. Integrity, on the other hand, signifies detection of any deliberate or accidental modifications to remote access communications that take place during transfer. Finally, availability signifies ensuring that users can utilise remote access to access resources whenever required (NIST, 2016). All elements of telework and solutions for remote access (e.g., client devices, internal servers, remote access servers) require to be secured against various threats to achieve these goals. These also frequently require further protection because their characteristics typically put them in a position where they are more exposed to external threats in contrast to technologies accessed only from within the organisation (NIST, 2016).

Prior to designing and implementing solutions for telework and remote access, system threat models should be developed by firms for the remote access servers and remotely accessed resources. remote access. The development of system threat models commences with identification of resources of significance and the possible dangers, susceptibilities, and security constraints associated with these resources. Following this, the probability of effective attacks and their consequences is quantified. Finally, this information is analysed to ascertain the location(s) where there is a need to improve or enhance security controls. Organizations are helped by threat modelling to recognise security needs and to create the solution for remote access to integrate the necessary controls to fulfil the security needs. Significant security challenges for these technologies that most telework threat models would incorporate include: lack of physical security controls, unsecured networks, infected devices on internal networks, and external access to internal resources (NIST, 2016).

2.5 Virtual Private Networks

A VPN is a networking technology that uses the Internet to connect one or more computers to a private network. These networks are used by businesses to permit their workers to remotely access corporate resources that they would not otherwise be able to from their homes, hotels, etc. (Chávez, 2020).

A VPN can be described as “an encrypted connection over the Internet from a device to a network” (CISCO, 2022). The encrypted connection assists in ensuring the safe transmission of sensitive data. It checks unapproved people from “eavesdropping on the traffic” and permits the user to perform work from a remote location. VPN technology is commonly utilised in corporate settings (CISCO, 2022).

The NIST (NIST, no date) provides the following different definitions of VPN:

- “Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line.”
- “Protected information system link utilizing tunneling, security controls … and endpoint address translation giving the impression of a dedicated line.”
- “A virtual network built on top of existing networks that can provide a secure communications mechanism for data and IP information transmitted between networks.”
- “A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network.”

- "A virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and IP information transmitted between networks or between different nodes on the same network."

VPNs safeguard communications performed over public (E.g., Internet) and private networks (e.g., fibre networks, Multiprotocol Label Switching (MPLS) networks). VPNs can offer different forms of data protection such as, replay protection, confidentiality, data origin authentication, integrity, and access control (Barker *et al.*, 2020).

Network Layer Security

Internet Protocol Security (IPsec) is a group of "open standards" for safeguarding private communications over public networks. IPsec is the most common security control for network layer and is general utilised to encrypt IP (Internet Protocol) traffic between a network's hosts and to generate a VPN. IP networking is the global standard utilised to offer communications on a network. The approximate composition of IP communications is as four layers that function together. Data is delivered across intermediate layers from the highest layer to the lowest layer when a user desires to transmit data through networks, with additional information being added by each layer. The accumulated data is sent through the physical network by the lowest layer. Subsequently, the data is transmitted to its destination across the layers. In essence, the data a layer produces are condensed in a bigger container by the preceding layer. Table 2.6 summarises the functions of the four IP layers.

Table 2.6:
IP Layers (Barker *et al.*, 2020, p. 3)

Layer	**Description/Function**
Application Layer	Transmits and collects data for specific applications, including • Domain Name System (DNS),

Layer	**Description/Function**
	• web traffic (through the Hypertext Transfer Protocol (HTTP) and HTTP Secure (HTTPS)), and • email (using Simple Mail Transfer Protocol (SMTP) and the Internet Message Access Protocol (IMAP))
Transport Layer	Offers services (connection-oriented or connectionless) for transporting services related to the application-layer between networks. Optionally, the transport layer can guarantee the trustworthiness of communications. Protocols commonly utilised by this layer are: • Transmission Control Protocol (TCP), which offers dependable connection-oriented communications, and • User Datagram Protocol (UDP), which offers undependable connectionless communications
Network Layer	Guides packets across networks. Protocols commonly utilised by this layer are: • IP (Internet Protocol) which is the basic network layer protocol for TCP/IP, • Internet Control Message Protocol (ICMP), and • Internet Group Management Protocol (IGMP)
Data Link Layer	Deals with communications between the physical elements of the network. Protocols commonly utilised by this layer are: • Ethernet and the various Wireless Fidelity (WiFi) standards. For instance, 802.11 of the Institute of Electrical and Electronics Engineers (IEEE).

Each IP layer has security controls for network communications. This is because data is transmitted from the highest layer to the lowest layer with more information being added by the intermediate layers. Consequently, security constraints at a higher level are not sufficient to offer complete protection for the following layers since higher layers are unaware of the functions of the lower layers. The application layer, for instance, requires the establishment of separate controls for every application. However, it must be noted that controls at the application layer can safeguard application data. However, they cannot safeguard communication metadata since this information is present at a lower layer. Controls at the application layer for safeguarding network communications should, whenever feasible, be solutions based on standards that have been utilised for some time. For instance, the Secure/Multipurpose Internet Mail Extensions (S/MIME), which is typically employed to encrypt email messages, and the Secure Shell (SSH) protocol, which scrambles remote login sessions. Controls at the transport layer can be utilised to safeguard the data in a specific communication session among two hosts, frequently termed a netflow. Transport layer controls cannot safeguard IP information as this is added at the network layer. Currently, the best practice as regards protocols to safeguard varied netflows are to utilise Transport Layer Security (TLS) to safeguard TCP streams and Datagram Transport Layer Security (DTLS) to safeguard UDP datagrams (Barker *et al.*, 2020).

Controls at the network layer are applicable to all applications. That is, they are not specific to any application. For instance, this layer can protect all network communications between two networks or hosts without applications being modified on the servers or the clients. Network layer controls (e.g., IPsec) offer a more robust solution than controls in the transport or application layer because of the challenges, in many environments, in adding restrictions to individual applications. In addition, network layer controls offer a means for network administrators to impose specific security policies. A further benefit of network layer controls is that they can safeguard the data inside the packets together with each packet’s IP information since this layer adds IP information (e.g., IP addresses). However, controls at the network layer offer lower flexibility and control for safeguarding certain applications than controls at the transport and application layers (Barker *et al.*, 2020).

Finally, controls at the data link layer are used with all communications on a certain physical link. For instance, a reserved circuit connecting two buildings or a WiFi network. For reserved circuits, data link encryptors which are specialized hardware devices are the most frequent providers for data link layer controls. On the other hand, for WiFi networks, data link layer controls are typically offered by means of WiFi chipset firmware. Data and IP information can both be protected by controls at this layer since it is beneath the network layer. Controls at the data link layer are easier to implement since they are comparatively simple in contrast to the other layer controls. Furthermore, they support IP and other network layer protocols. Since controls at the data link layer are exclusive for a certain local WiFi signal or physical link, they are inappropriate for safeguarding links to remote endpoints, such as setting up a VPN over the internet (Barker *et al.*, 2020).

In general, an internet-based connection comprises many physical connections attached together. Using data link layer controls to safeguard such a connection would require the participation of several parties and varied protocols for each element of the physical chain. Hence, it is simpler to regard the internet to be unreliable as a whole and employ controls at the preceding layers (i.e., network, transport, or application). The principal use of data link layer protocols has been to offer further protection for certain physical connections that are not reliable (Barker *et al.*, 2020).

IPsec Protocol

IPsec has become the network layer security control most commonly utilized for safeguarding communications. It is a charter of open standards for safeguarding private communications over IP networks. IPsec can offer any blend of different types of protection depending on the manner in which it is implemented and configured. The different types of protection include confidentiality, integrity, confidentiality and integrity, peer authentication, replay protection, traffic analysis protection, access control, perfect forward secrecy (PFS), and mobility (Barker *et al.*, 2020). From the perspective of confidentiality, IPsec ensures that unauthorised parties cannot discover data by utilising a cryptographic algorithm and a secret key to encrypt and decrypt data. The value of the secret key is known only to the participants exchanging data. From the perspective of integrity, IPsec ascertains if the data has been deliberately or accidentally changed during transit. Data integrity can be guaranteed by producing a MAC (message authentication code) value. This is a cryptographic checksum (hash) of the data produced with a secret key (does not correspond to the secret key utilised in encryption) which is agreed upon mutually. Confidentiality and integrity can be integrated into one Authenticated Encryption with Associated Data (AEAD) algorithm which utilises a sole secret key instead of two distinct keys to integrate cryptographic checksums and symmetric encryption into one process. Both parties continue to be required to possess the same secret key and utilise the same associated data. As regards peer authentication, each IPsec endpoint verifies the identity of the other IPsec endpoint with which it desires to communicate, confirming that the network data and traffic are only sent to the validated and anticipated endpoint. In replay protection, the same data is not accepted several times, and is not accepted when it is completely out of sequence. This blocks attackers from duplicating and resending authorised IPsec encrypted data for evil reasons. IPsec's tunnel mode provides traffic analysis protection when it is used. In this, a person supervising network traffic is unaware of the parties in communication, how frequently the communications are taking place, or the quantity of data being exchanged. Concerning access control, filtering can be performed by IPsec endpoints to confirm that certain network resources can be accessed only by validated IPsec users. For PFS, session keys are created by IPsec endpoints that are modified often, usually every hour. Later, the old session keys are wiped by the endpoints from volatile memory. In addition, no copies of the private decryption keys are left with any of the entities. Finally, with regard to mobility, an endpoint's outer IP address can change without causing the encrypted data flow to be interrupted. Since the application uses the inner (encrypted) IP address to communicate, it is not affected by changes to the outer IP address. This permits a device to switch between WiFi, Ethernet, or mobile data without interruptions to the application (Barker *et al.*, 2020).

VPN as an implementation of IPsec

The provision of VPN services is the most common usage of IPsec implementations (Barker *et al.*, 2020). As mentioned previously, a VPN is a “virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and IP information transmitted between networks or between different nodes on the same network” (Barker *et al.*, 2020, p. 8). A VPN can assist in the safe transmission of sensitive data across public networks since it can be utilised over existing networks, such as the internet. Frequently, this is cheaper than options such as reserved private telecommunication links between firms or branch offices. Since reserved private lines are frequently multi-tenant solutions themselves, they are nowadays typically safeguarded by an IPsec VPN. Flexible solutions are offered by remote access VPNs including, safeguarding communications between remote workers and the servers of an organization. A VPN can be setup in a single network to safeguard communications that are particularly sensitive from other participants on the same network. It can even use a mesh of IPsec connections among all the nodes in one network to ensure that no unencrypted data ever emerges on the network (Barker *et al.*, 2020).

The following cryptographic security services are provided for VPNs by IPsec:

- Confidentiality
- Integrity
- Establishment of shared secret keys
- Peer authentication
- Deployment risks

The principal VPN architectures based on IPsec include:

- *Gateway-to-gateway*. This architecture safeguards communications between two exact networks. For instance, the main office network of a firm and network of a branch office or the networks of two business partners (Figure 2.6) (Barker *et al.*, 2020).

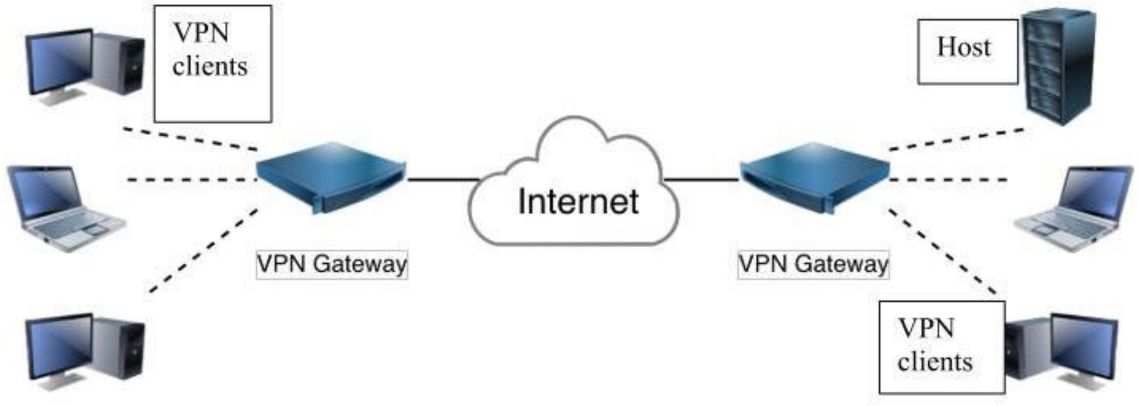

Figure 2.6:
Example of Gateway-to-gateway VPN architecture (Barker *et al.*, 2020, p. 12)

- *Remote* access or *host-to-gateway*. This architecture safeguards communications between individual hosts and a particular network owned by an organization. This architecture is utilised most frequently to permit hosts on unsecured networks (e.g., traveling employees and teleworkers) to obtain access to services internal to the organisation, *such* as the email and web servers of the organisation (Figure 2.7) (Barker *et al.*, 2020).

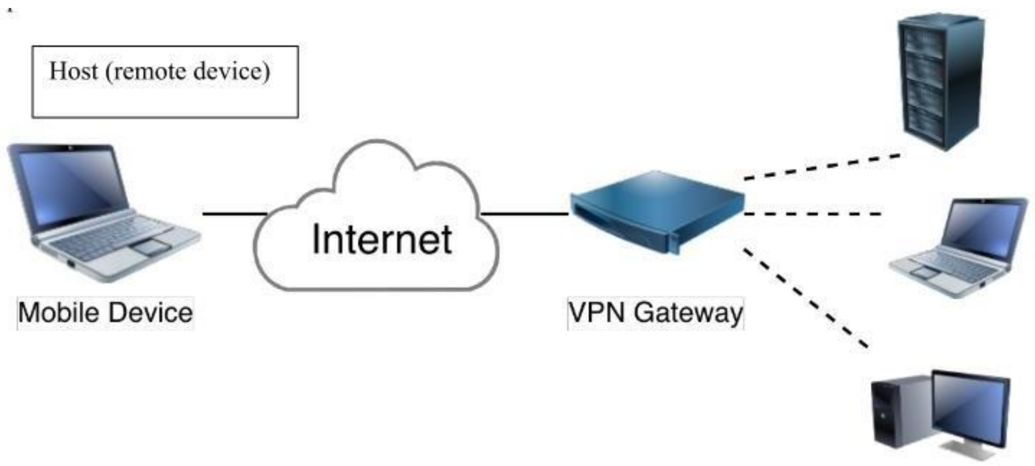

Figure 2.7:
Example of remote access VPN architecture (Barker *et al.*, 2020, p. 13)

- *Host-to-host*. This architecture safeguards communication between two definite computers. It can be utilised when a remote system that needs the usage of protocols that are fundamentally insecure is needed to be used or administered a by a few users (Figure 2.8) (Barker *et al.*, 2020).

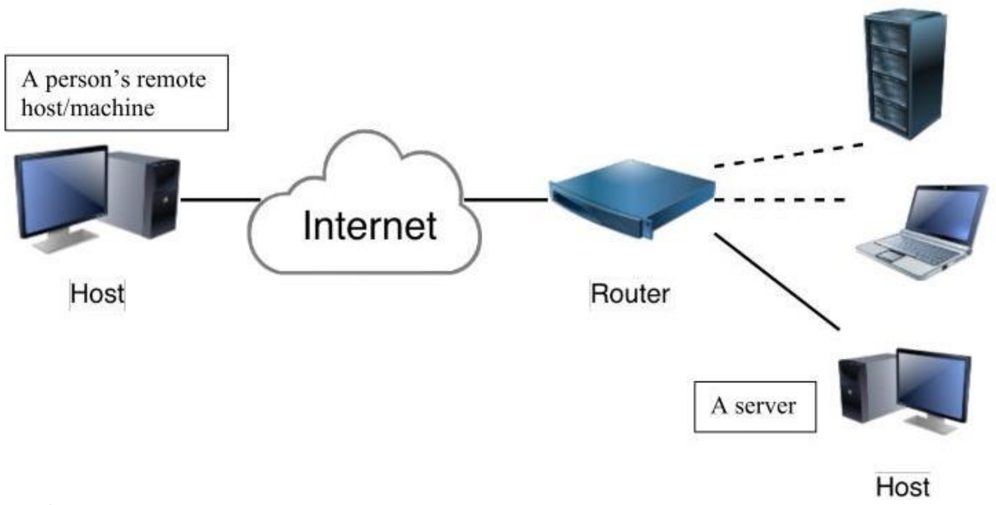

Figure 2.8:
Example of host-to-host VPN architecture (Barker *et al.*, 2020, p. 15)

- *Mesh*. In this architecture, several hosts inside one or a small number of networks all set up individual VPNs with one another (Barker *et al.*, 2020).

2.6 Technology support for teleworking

A recent study by Adame (2021) investigated the solution derived by the IT Department of a water utility company to successfully manage and safeguard their endpoints in the context of teleworking. While endpoints typically signify devices that are connected physically to a network, in the teleworking context this was extended to include PCs, laptops, and iOS devices that were utilised by employees to access the resources of the firm while functioning outside the organisation's network. The concerns of the IT department as regards their responsibility towards management of these endpoints included provision of software updates and deployments, support for operating system, and remote troubleshooting or support. In addition, the department was anxious about their capacity to adequately confirm compliance of the endpoints and offer sufficient protection from threats (Adame, 2021). The organisation's solution was to use different Microsoft cloud-based services such as, Microsoft Azure Active Directory, Intune, a Cloud Management Gateway, Endpoint Manager, and Microsoft Defender for Endpoint, to facilitate the IT department's fulfilling of their responsibilities in the novel telework setting. In addition, the organisation used on-site infrastructure management technology such as, VPN, Active Directory, Microsoft Endpoint Configuration Manager, and Group Policy. This study provided some insights regarding the probable challenges of organisations that support telework specifically as regards regulating information flow and bringing about zero trust. Zero Trust was defined by the National Institute of Standards and Technology (NIST) as "an evolving set of cybersecurity paradigms that moves defenses from a static, network-based perimeters to focus on users, assets, and resources" (Rose *et al.*, 2020, p. ii).

Golden (2009) highlighted that mobility was the inherent aspect of telework. That is, a person can work from almost anywhere. This is supported by an enhanced dependence on technology to perform work activities. He noted that while this technology was context-specific, it typically required computers with software specific to the job, phones, other electronic devices, and remote access at high-speed to corporate databases.

2.7 Research Gap

Overall, this review of literature has revealed that the focus on productivity in teleworking and cybersecurity through VPN use in relation to teleworking appears to be limited and often skewed with researchers focusing on such varied aspects as, user perspectives, underlying technology, risks of using VPN, and frameworks. There is also an apparent demarcation of focus, as some researchers focus exclusively on the productivity aspects of teleworking whereas others focus exclusively on facets of VPN. There is hence a lack of empirical research related to the experiences of organisations with regard to the switch to teleworking during the pandemic, the consequent impacts to their security and productivity, and their plans for the future.

Consequently, a comprehensive examination of an organisation's experience with VPN usage in the teleworking scenario engendered by Covid-19 would help technologists and practitioners to finetune not only the technological aspects of VPN but also processes and policies to implement VPN in organisations with the intent of balancing productivity and cybersecurity, which is the objective of the present study.

2.8 Preliminary Conceptual Framework

The insights from the literature review suggest a preliminary conceptual framework for productivity and cybersecurity through VPN usage in organisations supporting teleworking (Figure 2.9). The framework builds on the basic elements of the telework/telecommuting success model (Siha and Monroe, 2006, p. 472) and interposes these with facets of telework, impacts of telework, and VPN usage. The telework/telecommuting success model was utilised as the underlying model in the study due to its acknowledgment that technology enables and indeed is the mainstay of teleworking. The empirical components of the study which follow will use this preliminary framework as their basis.

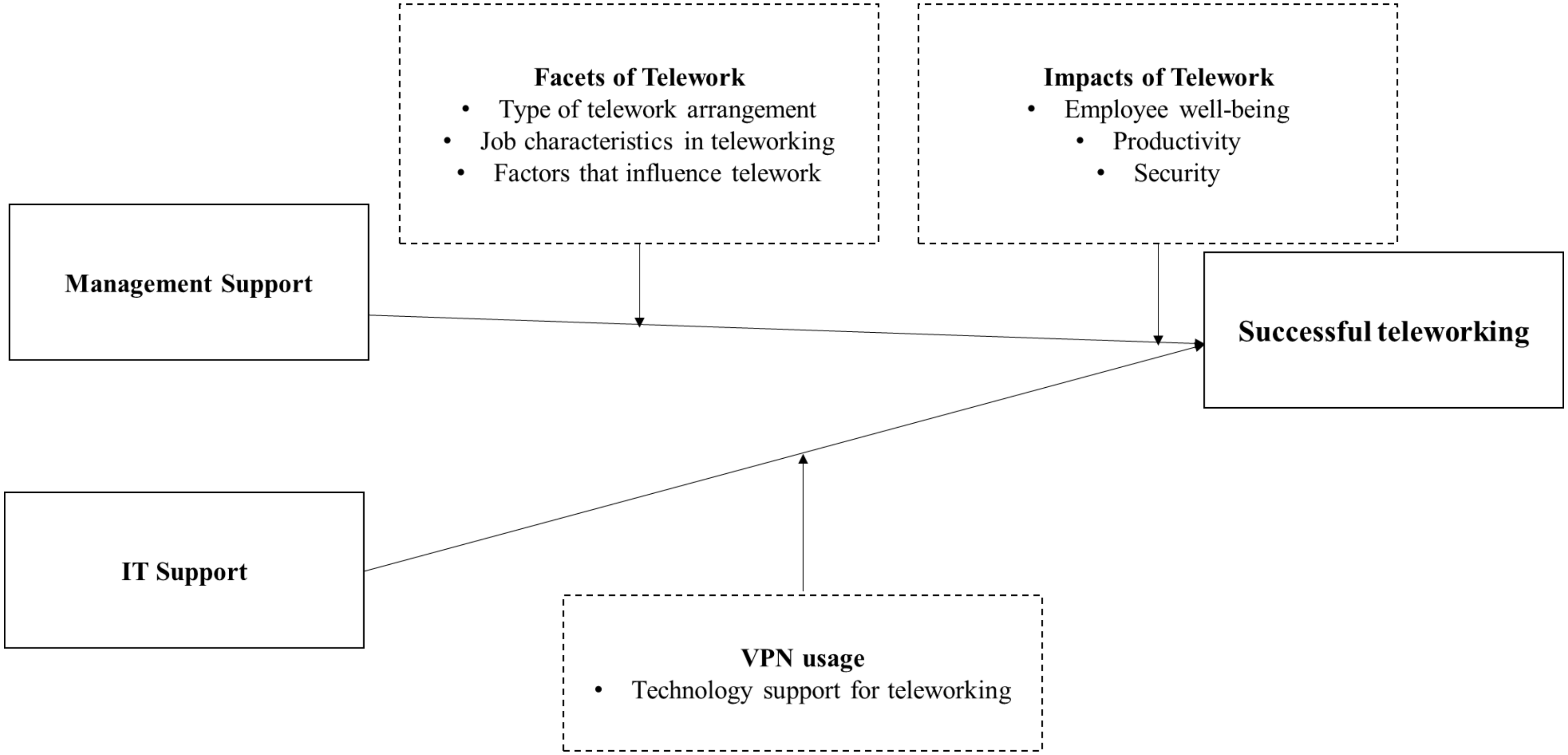

Figure 2.9
Preliminary visualisation of conceptual framework for productivity and cybersecurity during teleworking through VPN usage

2.9 Summary

This chapter reviewed recent research related to telework and teleworking, the types of telework arrangements, job characteristics in teleworking, and factors that influence telework. In addition, research related to the impacts of teleworking on employee well-being, efficiency and productivity, and security was reviewed. Furthermore, this chapter included research on VPNs and the role of technology to support teleworking. The chapter concluded by summarising the perceived research gap and by providing the preliminary conceptual framework for productivity and cybersecurity through VPN usage in the continued use of teleworking in organisations based on the review of literature.

CHAPTER III:
METHODOLOGY

3.1 Chapter Introduction

The continued inclination of employees to telework even in the post-pandemic scenario indicates that it is necessary to perform a thorough investigation of the experiences of organisations which have been supporting teleworking employees and utilising different approaches to ensure productivity and cybersecurity. In this regard, the researcher believed that a case study approach would be most suitable for such a study as it would help obtain in-depth data regarding the impact of VPN solutions on the productivity and security of an organisation.

The purpose of this chapter is to provide an overview of the methodology utilised in this study. That is, an overview will be provided of the research paradigm, research design, research approach, and ethical considerations, pertaining to the research.

3.2 Research paradigm

The selection of the most suitable research method for a study entails consideration of the type(s) of information required to answer the study's research questions (Newell and Burnard, 2011). The selection of method together with the study's design and objectives on the whole, however, are impacted also by the researcher's ontological and epistemological viewpoints (Richards and Morse, 2013). In other words, the commencement of this study was influenced by the researcher's preliminary viewpoints and beliefs regarding the world, the forms of knowledge regarding that world and freedom of individuals as regards external aspects. These beliefs relate to the assumptions of the research regarding the nature of the universe, in general, and the matter being researched, in particular (or ontology), the form of knowledge about this universe (or epistemology), and the nature or character of humans. These, together, comprise the research paradigm, that is, “conceptual lens through which the researcher examines the methodological aspects of their research project to determine the research methods that will be used and how the data will be analysed” (Dekkers, Carey and Langhorne, 2022, p. 76).

Ontology signifies the view or suppositions of the researcher regarding the basic character of reality. For instance, whether reality exists autonomously and can be recognised and evaluated using methods comparable to the physical universe, or whether reality can only be recognised and interpreted through the methods in which it is formed in the minds of the persons encountering it. Three orientations are commonly explored in case study research. The first, the constructivist/interpretivist/relativist ontological paradigm utilised by Stake (2013) presupposes that the reality of societal phenomena is neither objective nor independent but instead is formed by societal processes and the interpretation that individuals ascribe to their encounters with them (Seal, 2012; Burr, 2015). This approach places emphasis on the experiences of an individual the researcher’s understanding of these to derive an understanding of the phenomenon from the data itself (Harrison *et al.*, 2017). This is in contrast with the positivist/postpositivist/realist ontological paradigm utilised by Yin (2018) where the principles of objectivity and generalizability of outcomes are embraced (Ellingson, 2013). This paradigm depends entirely on collection of quantitative data. The third is the pragmatic constructivist approach utilised by Merriam (Merriam and Tisdell, 2016). This approach utilises a combination of qualitative and quantitative approaches and an extremely organised approach to collect and analyse data. Case studies may be viewed by researchers who follow a “social constructive or interpretive research philosophy” as a means to scrutinise a “phenomenon embedded within a unique situation at a certain point in time” (Ward and Street, 2010, p. 800). A social constructive approach focuses on "human social processes and activities that are considered both reflexively transformative and self-sustaining, rather than objective artifacts, things, or substances, as phenomena of interest" (Maréchal, 2010, p. 224). Consequently, in this perspective it is acknowledged that individuals develop their own individual understandings and implications of the world on the basis of their experiences (Seal, 2012; Merriam and Tisdell, 2016; Creswell and Creswell, 2018). From this perspective, individuals within an organisation may have different experiences with teleworking and their education, role, experience, etc., may influence the manner in which they make sense of their working universe and consequently construct a reality from this (Berger and Luckmann, 2016). Performing research in this paradigm requires the researcher to examine the different ways in which persons encounter social experiences and their interpretation of their experiences together with the factors that impact these interpretations.

Relatedly, epistemology refers to "assumptions about knowledge, what constitutes acceptable, valid and legitimate knowledge, and how we can communicate knowledge to others" (Saunders, Lewis and Thornhill, 2019, p. 133). In contrast to ontology which may appear to be rather conceptual, epistemology is more obviously relevant as the adoption of an epistemology depends on the forms of knowledge available (Saunders, Lewis and Thornhill, 2019). Simply stated, epistemology signifies the manner in which knowledge regarding a phenomenon can be obtained (Cooksey and McDonald, 2019). Two principal paradigms are associated with epistemology namely, positivism and interpretivism (Bryman, 2012). Positivism "advocates the application of the methods of the natural sciences to the study of social reality and beyond" (Bryman, 2012, p. 28). In contrast, interpretivism is "predicated upon the view that a strategy is required that respects the differences between people and the objects of the natural sciences and therefore requires the social scientist to grasp the subjective meaning of social action" (Bryman, 2012, p. 30).

The positivist epistemology presupposes that the societal universe can be studied using methods comparable to the natural world because it has an unbiased realism external to the views of individuals. This approach is associated with quantitative techniques of research such as, structured questionnaires and the usage of statistical approaches to scrutinise variables and evaluate associations among them (Newell and Burnard, 2011). The interpretivist epidemiology, in contrast, presupposes that societal truths are varied and biased in character. Moreover, they are constructed socially in the intellects of the persons who experience them and they reflect the setting in which they take place. According to this approach, awareness of societal phenomena can be gained only by scrutinising the experiences and viewpoints of individuals in the specific setting wherein they take place utilising qualitative approaches such as, focus groups or in-depth interviews (Newell and Burnard, 2011; Bryman, 2012; Stake, 2013). A further epistemological perspective is the pragmatic paradigm (Creswell and Plano Clark, 2018). This paradigm is utilised by many researchers and places emphasis on practicality. That is, the emphasis of researchers is on the outcomes of the research and accordingly their data collection focuses on the principal significance of the research question instead of the research approaches being used (Creswell and Plano Clark, 2018). From a philosophical perspective, pragmatism is associated with mixed methods research which can be described as "the class of research where the researcher mixes or combines quantitative and qualitative research techniques, methods, approaches, concepts or language into a single study" (Johnson and Onwuegbuzie, 2004, p. 17).

3.3 Research Design

A mixed-methods, single case, case study research design was adopted for the study to permit deeper scrutiny of the matter of teleworking in a single organisation. Case study research designs utilising a variety of methods for data collection are robustly associated with the constructivist epistemological approach as they help a researcher to investigate a phenomenon within the context it occurs in naturally. Further, it helps to investigate the manner in which this context impacts opinions or encounters associated with the phenomenon (Stake, 2013). The usage of many research approaches and sources of data permits the researcher to gain awareness of the way research participants interpret their experiences and also aid in the researcher's own understanding of these during the course of the research. Yin (2014, p. 18) defines the case study as:

> "an empirical inquiry that investigates a contemporary phenomenon (the "case") in depth and within its real-world context, especially when the boundaries between phenomenon and context may not be clearly evident"

The approach is suitable in settings where a complete explanation of the topic being researched cannot be provided by a single report. It is appropriate for accomplishing profound, all-inclusive awareness of extensive, multi-faceted happenings and in gaining awareness of collaborative processes, associations, political matters, and influence strategies in certain settings (Lewis and Nicholls, 2014; Marshall and Rossman, 2016).

As also highlighted by Crowe and colleagues (2011, p. 1), the case study approach is useful when it is necessary to obtain an "in-depth appreciation of an issue, event or phenomenon of interest, in its natural real-life context." The approach is utilised when there is a requirement to obtain profound understanding of a certain event or occurrence in a certain everyday setting, "especially when the boundaries between the phenomenon and context are not clearly evident" (Yin, 2014, p. 13).

Three types of case studies are typically utilised in research: exploratory, descriptive, and explanatory. An exploratory case study scrutinises a case(s) to obtain deeper understanding whereas a descriptive case study describes the features of a case. The explanatory case study approach attempts to answer "how" and "why" questions as regards the case (Yin, 2018). This study uses an exploratory and descriptive case study of a single organisation to investigate the processes, policies, risks, challenges, benefits, etc., of using VPN to support productivity and ensure cybersecurity. This combination of case study approaches is suitable for the study because the researcher wanted to learn from the experiences of organisations as regards productivity of teleworking employees and security when VPN is used. In addition, the researcher wanted to investigate the features of such organisations.

In addition, the researcher decided to use a pragmatic approach (Merriam and Tisdell, 2016). By using this approach, the researcher acknowledged that the research questions determine the methodology most suitable for the study. A combination of methods was also deemed suitable. Mixed methods is "a research paradigm that combines specific positivistic elements of quantitative research methods with specific constructivist elements of qualitative research methods. Generally, this approach can be sequential or parallel, with the quantitative and qualitative approaches used alternately or together to investigate the same phenomenon" (Kitchenham, 2010, p. 561).

3.4 Rationale for Selection of the Case Study Design

The case study approach is a relevant methodological choice when the research questions of a study attempt to explain the functioning of a social phenomenon or when an extensive or profound explanation of such a phenomenon is required (Yin, 2018). Case studies allow a researcher to concentrate extensively on a "case" and to preserve a rounded and practical viewpoint, as in the case of, for example, managerial and organizational processes, life cycles of individuals, behaviour of small groups, changes to neighbourhoods, performance in school, transnational relations, and industry maturation (Yin, 2018). Furthermore, the use of the case study approach helps the researcher design the research to suit both the case and underlying research question(s) (Hyett, Kenny and Dickson-Swift, 2014). Relatedly, the methodology's robustness is also evident in its flexibility to encapsulate the intricacy of the event or occurrence being investigated while considering the context in which it takes place (Hyett, Kenny and Dickson-Swift, 2014). Additionally, research rigour can be accomplished by using triangulation of methods. This enables researchers to gain a rich awareness of a phenomenon by using multiple perspectives to obtain profound insights regarding the case (Hercegovac, Kernot and Stanley, 2020).

Thus, the overarching research methodology used in the study is a case study. The design of the case study was based on the concept of mixed methods which follows the concept of convergent parallel design. The principal purpose of the convergent parallel design is to collect and analyse data in parallel using a combination of qualitative and quantitative approaches (Creswell and Creswell, 2018; Creswell and Plano Clark, 2018). Figure 3.1 depicts the overall case study design for the study.

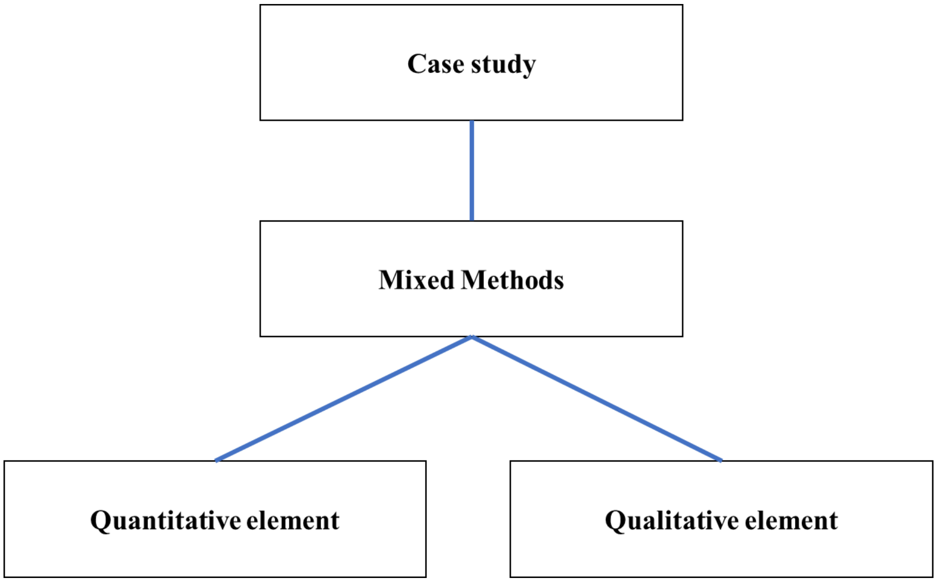

Figure 3.1
Case Study Design for the study (Guetterman and Fetters, 2018, p. 901)

The research question of the study, *Can productivity and security be achieved in the teleworking scenario in the post-COVID context through the usage of VPN?*, specifically its character and the motivating ontological and epistemological beliefs together with the necessity to accomplish in-depth analysis, supported the option of performing a *single* case study. Specifically, a *holistic* single case (Yin, 2014) study approach was chosen as there would be only a single unit of analysis: the case organisation. That is, an organisation where the teleworking could have had an impact on employees' productivity and organisational security. In addition, the case organisation was deliberately *broad*. That is, instead of focusing on a specific department, the researcher believed that it would be more relevant to choose employees across locations, levels, and encompassing the whole organisation.

3.5 Research Approach

Sampling Strategy

Typical sampling strategies in research include probability, purposive, and convenience sampling (Teddlie and Yu, 2007). The principal use of probability sampling techniques is in studies with a quantitative orientation and involve “selecting a relatively large number of units from a population, or from specific subgroups (strata) of a population, in a random manner where the probability of inclusion for every member of the population is determinable” (Teddlie and Tashakkori, 2009, p. 152). The aim of probability samples is to achieve representativeness. That is, to achieve the extent to which the entire population is accurately represented by the sample. On the other hand, the primary use of purposive sampling techniques is in qualitative studies. This technique may be described as “selecting units (e.g., individuals, groups of individuals, institutions) based on specific purposes associated with answering a research study’s questions” (Teddlie and Yu, 2007, p. 77). Convenience sampling entails obtaining samples that are easily accessible and also ready to take part in a study (Teddlie and Yu, 2007).

In contrast, sampling strategies in mixed methods research typically involve the usage of both probability and purposive sampling methods. The focus of the sampling is to produce a sample that will deal with the study’s research questions. Moreover, there will be multiple samples which vary in size based on the strand of research. Additionally, both quantitative and qualitative data are produced (Teddlie and Yu, 2007). The sampling approach utilised in the study was deemed suitable and applicable as it ensured that a variety of participants participated in the study. In this study, employees across the case organisation were involved in the quantitative strand. Employees from the IT/IS departments and executives involved in decision-making were involved in the qualitative strand.

Overall, the sampling for the study was at two levels. First, the case organisation was chosen and second, participants within the case organisation were chosen for participation in the quantitative and qualitative strands.

Sources of data for the study

Various sources of data are associated with case studies such as, documents, archival records, physical artifacts, observation of participants, direct observation, and interviews (Yin, 2018). Prior research has indicated that the usage of multiple sources strengthens a case study. In fact, a case study can be considered to be a special strategy of research that can combine quantitative and qualitative approaches. Moreover, the usage of multiple sources facilitates triangulation. In other words, the data obtained from various sources can be compared which enhances the reliability and validity of the study (Mills, Durepos and Wiebe, 2010).

Within the case study, the researcher used both primary and secondary sources of data. Primary data, here, signifies data that the researcher collected directly. Secondary data signifies data obtained from published academic and business sources, company reports. That is, data not directly collected by the researcher.

Instruments of Research

Since the researcher required information related to the teleworking experiences of the firm from the perspectives of productivity of employees and security of the organisation's data and resources, multiple research instruments were adopted.

Employee Questionnaire

A questionnaire was designed for use with employees who teleworked and participation was on a voluntary basis (see Appendix B). The questionnaire contained four sections inspired by preliminary conceptual framework of the study (see Section 2.8). The first contained five questions related to the **demographic** details of the employees (age, gender, educational qualification, nature of employment, and work experience in the case organisation). The second section contained twelve questions related to the **teleworking experience** of the employees (duration of teleworking, teleworking before the pandemic, continuing to telework, who provides the facilities for teleworking, etc.). The questions in these two sections were close-ended and options were provided for the participants to choose their responses. The third section focused on **productivity while teleworking** and contained two questions. The first question was composed of 35 statements and measured the employees' opinion regarding features of their work such as, job role, job performance, work autonomy, and job complexity. The second question in this section contained 18 statements and measured the employees' opinion regarding facets of their productivity such as, perceived productivity, productivity level, and organization measure of productivity. The responses for this section of the questionnaire followed a 5-point Likert scale ranging from 5 - strongly disagree; 4 - disagree; 3 - neutral; 2 - agree to 1- strongly agree.

The focus of the fourth section of the questionnaire was **VPN and teleworking** and contained six questions. The first five questions in this section related to VPN used, why this was chosen, type of VPN subscription, reason for using a VPN product, and frequency of using VPN. The first question was open-ended and the remaining four questions in this section was close-ended and options were provided for the participants to choose their responses. The last question contained 27 statements related to the facets of using VPN such as, VPN and productivity, awareness of VPN concept, VPN functioning, VPN risks, and VPN advantages. The responses for this question followed a 5-point Likert scale ranging from 5 - strongly disagree; 4 - disagree; 3 - neutral; 2 - agree to 1- strongly agree. Figure 3.2 depicts the components of the questionnaire.

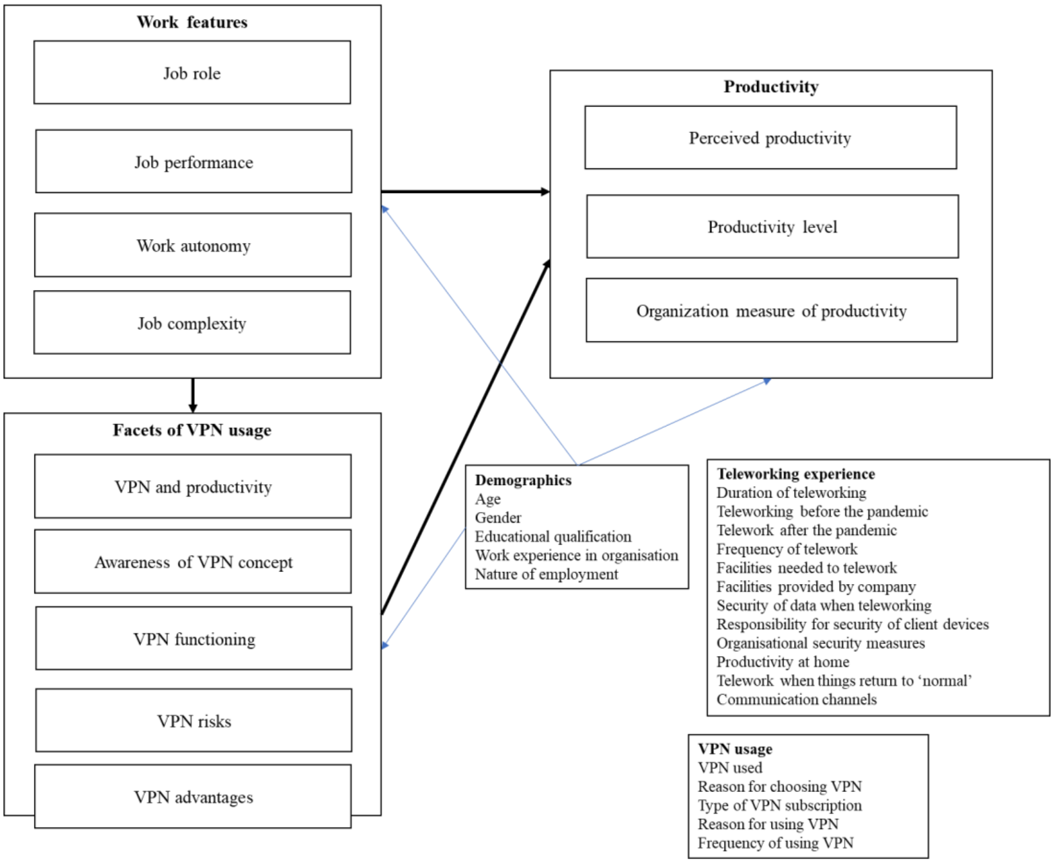

Figure 3.2
Components of the Questionnaire

Interviews

Interviews are required when an individual's behaviour, feelings, or interpretations of the surrounding universe cannot be observed (Merriam and Tisdell, 2016). A research interview can be defined as "a process in which a researcher and participant engage in a conversation focused on questions related to a research study. These questions usually ask participants for their thoughts, opinions, perspectives, or descriptions of specific experiences" (DeMarrais, 2004, p. 54).

In general, three kinds of approaches are associated with interviews: structured, unstructured, and semi-structured. These approaches differ in the questioning that takes places during the process of individual interviews as per the level to which the questioning is standardised or structured. Overall, a structured interview focuses on studying facts, an unstructured interview places emphasis on meaning, and a semi-structured interview concentrates on interpretation of narratives from a person in a certain situation (Qu and Dumay, 2011). Surveys are the most typical form of structured interviews as these are based usually on the research logic utilised by questionnaires. That is, "standardized ways of asking questions are thought to lead to answers that can be compared across participants and possibly quantified" (Brinkmann, 2014, p. 286). In contrast, unstructured interviews have "little preset structure" and the interviewer primarily listens to what the interviewee has to say without interrupting. On the other hand, semi-structured interviews are the most widespread form of interviewing and they allow the interviewer to interact with the interviewee and obtain more knowledge by following up on important lines of thought (Brinkmann, 2014). In the present study, the researcher decided to proceed with semi-structured interviews to ensure that the conversation during the interviews could be directed to issues relevant to the current research project.

Consequently, in addition to the questionnaire, two sets of interview schedules were created (see Appendix D) based on the preliminary conceptual framework. A semi-structured interview schedule is "simply the list of topics and associated questions that the interviewer asks the participant" (Bearman, 2019, p. 1). One interview schedule was designed for the management team. Sixteen questions relating to teleworking and productivity in teleworking were included in this schedule. The second interview schedule was designed for the IT/IS team and contained nineteen questions related to teleworking, security, and the use of VPN in teleworking. The rationale for including interviews was to obtain profound insights regarding the teleworking infrastructure and support provided the organisation, and the benefits and challenges associated with security and productivity due to the provision of teleworking.

Data collection

The interview schedules and questionnaire were used to obtain primary information from different stakeholders in the organisation such as, teleworking employees, personnel in the IT and information security departments, decision-making executives, etc. This combination of qualitative and quantitative approaches served as the triangulation of approaches to obtain different perspectives of the matter being considered.

Interviews were conducted with personnel in the IT and information security departments, and decision-making executives through zoom or telephone, as per the participants' preferences and reasons of practicality. Participants were reminded of the study's purpose, research procedures, their right to withdraw from the study at any time, and assurance of confidentiality as a first step in the interview process. The interviews were also audio-recorded, after receiving approval from the participants, to ensure that transcription could be complete (Merriam and Tisdell, 2016). The interviewer also made notes during the interviews to ensure that key points could be tracked and clarified, if required, later in the interview. Also, these could be useful during data analysis. The duration of the interviews was between 30 and 45 minutes.

In addition, the questionnaire was administered to 200 teleworking employees to obtain their perceptions regarding different facets of their teleworking experience and the support required from their organisation. The questionnaire was entered into a Google Form and sent to the preferred email addresses of participants.

Data Analysis

The primary data obtained using the questionnaire and interviews were analysed. The data from the questionnaire were analysed statistically. IBM's SPSS (Statistical Package for the Social Sciences) was utilised to perform the analysis. Relevant statistical tests such as descriptive statistics (averages and percentages, mean and standard deviation), t-tests (to identify the differences between the means of data when grouped using various criteria) and f-tests (to identify the F-distribution of the data), and Multivariate analysis of variance (MANOVA), to check whether different levels of independent variables, separately or in combination, have an impact on the dependent variables, were employed to obtain a meaningful interpretation of the collected data. Cronbach's alpha was used to test the reliability of the questionnaire and exploratory factor analysis (EFA) was used to test the validity of the questionnaire.

The data from the interviews were analysed qualitatively using thematic analysis (Boyatzis, 1998; Braun and Clarke, 2006). Since the preliminary conceptual framework was used as the basis of preparation for the interview schedules, the thematic analysis performed was essentially in two stages. The first stage was deductive or top-down in nature. In this form of thematic analysis, the categories are taken from an existing theory or conceptual framework (Proudfoot, 2022). Accordingly, the highest level of categories was already determined for the analysis namely, facets of telework, impacts of telework, and VPN usage. For this segment of the thematic analysis, Boyatzis' (1998) three-stage approach was used. The three stages are: firstly, to determine the themes "through reading and contemplation [of] the theory;" secondly, to check the "compatibility with the raw information" through pilot coding; and finally, "to determine the reliability of the coder" (Boyatzis, 1998, p. 36).

The second stage of thematic analysis was inductive or bottom-up in nature. In this approach, the process of thematic analysis commences by assigning codes to the data from the transcripts and then organising the codes into themes for scrutiny (Braun and Clarke, 2006). The interview transcripts were first read through to gain awareness of the facets of teleworking, productivity, and security. Second, all passages of the transcript were analysed by applying codes. After all the contents were coded, the codes were compared with each other, and higher-order categories were generated if any codes were associated with each other (Mannebäck and Padyab, 2021). The themes were then defined and assigned names. Finally, the analysis was reported (Braun and Clarke, 2006) following the quantitative results.

Timeframe of the research

This study was conducted between October 2022 and January 2023 in a cross-sectional timeframe. This study design was chosen since the identification of the case organisation, recruitment of participants, collection of data, followed by the data analysis and reporting will be completed at a single point of time.

3.6 Ethical Considerations

The research was conducted after taking the following several ethical matters into consideration:

- Informed consent was obtained from the participants. The participants were given a comprehensive overview of the research and given the opportunity to ask questions to confirm that they could provide their informed consent.
- Anonymity: The data obtained from the survey were anonymised to avoid recognisability of any information pertaining to individuals. Similarly, the

data obtained from the interviews were anonymised and no participant names or other details were utilised.

- Confidentiality: Participants were assured that their data would be kept confidential and utilised only for research purposes.

3.7 Chapter Conclusion

The purpose of this chapter was to provide an overview of the methodology utilised in this study. Consequently, the research paradigm underlying the study was discussed followed by a discussion of the research design. The rationale for the selection of the case study design was also provided. Details were then provided of the research approach such as, sampling strategy, sources of data for the study, instruments of research, data collection, data analysis, and timeframe of the research. Finally, the ethical considerations followed by the study were described.

CHAPTER IV:

RESULTS

4.1 Chapter Introduction

This chapter provides the outcomes of the analysis of the data collected for the study. As described in the previous chapter, the data obtained using the employee questionnaire were analysed using IBM's SPSS software. The outcomes of the statistical analysis are presented in this chapter. The interviews were analysed using thematic analysis (Boyatzis, 1998; Braun and Clarke, 2006) and the outcomes will be presented using the themes that collectively emerged from the interviews with members of the case study firm's management and IT teams. The chapter concludes with a summary of the results. The description of the case organisation is first provided.

4.2 Case Description

The case organisation was an Indian organisation listed on the National Stock Exchange of India (NSE), the Bombay Stock Exchange (BSE), and the New York Stock Exchange (NYSE). The core business of the firm was Consulting and IT services and the number of employees exceeded 100,000. In addition, the firm had more than 1,000 clients and the firm's annual revenues was greater than a billion USD.

The case organisation was selected using purposeful sampling which has been defined as "choosing subjects, places, and other dimensions of a research site to include in your research to enlarge your analysis or to test particular emerging themes and working hypothesis" (Bogdan and Biklen, 2007, p. 274). The global characteristics of the case organisation resulted in its selection. That is, the size and extent of organisation lent itself to the collection of various data at multiple levels such as, individual and sub-groups of individuals (Yin, 2014). Another aspect was the researcher's accessibility to the IT/IS and management teams. As mentioned in the description of the Methodology

(Chapter 3) for the study, employees across the case organisation were involved in the quantitative strand. Employees from the IT/IS departments and executives involved in decision-making were involved in the qualitative strand.

The researcher recruited the participants first for the qualitative strand. For the qualitative strand, the researcher used a contact in the IT/IS leadership to identify employees who had the necessary awareness and experience related to the implementation of teleworking in the organisation. The contact identified eleven potential interviewees, five from the IT/IS team and six from the human resources and delivery management teams. The researcher used the following inclusion criteria to shortlist participants for the interviews:

- Should be a member of IT/IS, human resources, or delivery management team
- Work experience of >10 years
- Willingness to participate in the study

The researcher reached out to the prospective interviewees via telephone calls and explained to them the purpose of the study and the plan for the interviews. He also assured them of confidentiality and anonymity. While eight of these individuals expressed their willingness to participate in the study, the schedules of only six (three from IT/IS team and three from the management team) could align immediately with the researcher's data collection schedule. The researcher then decided to proceed with the interviews with the initial six with the intention to follow up with the remaining individuals at a later time. However, the researcher found that there was sufficient information and no additional fresh information seemed likely after the six interviews were completed. Consequently, no further interviews were undertaken.

The researcher then used the services of the interviewees to recruit participants for the quantitative strand. Although the organisation has more than 100,000 employees, the researcher could gain access to only about 500 employees through this process. An email was sent to prospective participants with details about the study and a link to the questionnaire. Overall, 213 persons participated in the study. However, 13 questionnaires could not be used due to incomplete data, and the final number of participants for the quantitative strand was 200.

Overall, the number of participants for the qualitative and quantitative strands were deemed to be adequate as qualitative studies typically focus on a smaller sample of participants chosen for very specific objectives (Patton, 2015). Also, the researcher was aware that the findings from the case organisation could not claim to be generalisable to other organisations.

4.3 Findings from the questionnaire

Participant Demographics

The majority of the participants were aged between 31 and 40 years (54.5%) followed by those in the age group of 21-30 years (22.5%) and persons in the age group of 41-50 years (15.5%). The least number of participants (7.5%) were aged over 50 years (Table 4.1).

Table 4.1
Participants' Age

Age	Frequency	Percentage
21-30 years	45	22.5
31-40 years	109	54.5
41-50 years	31	15.5
51-60 years	15	7.5
Total	**200**	**100.0**

The majority of the participants were male (58.0%) and the remainder were female (42.0%) (Table 4.2).

Table 4.2
Participants' Gender

Gender	Frequency	Percentage
Male	116	58.0
Female	84	42.0
Total	**200**	**100.0**

The majority of the participants were Graduates (83.5%) followed by persons with Diplomas (7.0%), persons with Masters (5.5%), and persons with Doctorates (4.0%) (Table 4.3).

Table 4.3
Participants' Educational Qualification

Educational Qualification	Frequency	Percentage
Graduate	167	83.5
Masters	11	5.5
Doctorate	8	4.0
Diploma	14	7.0
Total	**200**	**100.0**

The majority of the participants had worked for <20 years (84.5%) in the organisation with largest number in this group being persons with <5 years (34.5%) in the organisation. A smaller group (15.5%) had worked in the organisation for more than 20 years (Table 4.4).

Table 4.4
Participants' Work experience in organisation (years)

Work experience (years)	Frequency	Percentage
<5	69	34.5
>5-10	58	29.0

Work experience (years)	Frequency	Percentage
>10-20	42	21.0
>20-30	24	12.0
>30	7	3.5
Total	**200**	**100.0**

The nature of employment for the majority of the participants was full time (85.0%). Of the remainder, 10% were part-time employees, 3.0% were contractors, and 2.0% were interns (Table 4.5).

Table 4.5
Participants' Nature of Employment

Nature of Employment	Frequency	Percentage
Full time	170	85.0
Part-time	20	10.0
Contractor	6	3.0
Intern	4	2.0
Total	**200**	**100.0**

Teleworking Experience

The majority of the participants had commenced teleworking only during COVID (98.5%). The remaining 2.5% had been teleworking for more than 2 years (Table 4.6).

Table 4.6
Participants' duration of teleworking

Duration of teleworking	Frequency	Percentage
Only commenced during COVID (i.e., <2 years)	197	98.5
2 – 5 years	2	1.0
>5 years	1	0.5
Total	**200**	**100.0**

Prior to the pandemic, the majority (98.5%) of the participants had not been teleworking (Table 4.7).

Table 4.7

Participants' experience of teleworking before pandemic

Teleworking before the pandemic	**Frequency**	**Percentage**
Yes	3	1.5
No	197	98.5
Total	**200**	**100.0**

After the pandemic, the majority (77.0%) of the participants had continued to telework (Table 4.8).

Table 4.8

Participants' experience of teleworking after the pandemic

Telework after the pandemic	**Frequency**	**Percentage**
Yes	154	77.0
No	46	23.0
Total	**200**	**100.0**

The majority of these participants (66.0%) were teleworking 3 days a week or less (Table 4.9). This could be due to a mandate from the firm for employees to be in the office for a specified number of days. The 10.0% who teleworked 4 days a week may have been granted an exception.

Table 4.9

Participants' number of days doing telework

Number of days doing telework	**Frequency**	**Percentage**
1 day a week	34	17.0
2 days a week	52	25.0
3 days a week	48	24.0
4 days a week	20	10
Total	**154**	**77.0**

The majority of the participants (70.5%) reported that the facilities for teleworking were provided by the organisation (Table 4.10). About one-fourth of the participants (26.5%) reported that they used a combination of facilities purchased by themselves or the firm. A very small number (3.0%) used facilities purchased by themselves.

Table 4.10

Provision on facilities for telework

Provision of facilities to telework	**Frequency**	**Percentage**
My company	141	70.5
I use facilities purchased by me	6	3.0
I use a combination of facilities purchased by me/provided by the company	53	26.5
Total	**200**	**100.0**

The facilities provided by the firm included personal computers for all employees and secure connectivity for the majority (71.0%). However, it appeared that the participants used their own mobile devices. Also, remote desktop access was not provided to all the employees. This may be due to the nature of the work (Table 4.11).

Table 4.11

Facilities provided by company

Facilities provided by company	**Yes (%)**	**No (%)**
Personal computers (desktop, laptop)	200 (100.0)	0 (0.0)
Mobile devices (smart phones, tablets)	3 (1.5)	197 (98.5)
Remote desktop access	22 (11.0)	178 (89.0)
Secure connectivity	142 (71.0)	58 (29.0)

The employees were also asked what they felt about the security of their data when teleworking (Table 4.12). It could be seen that the majority (52.5%) believed that their data were very secure whereas nearly equal numbers believed that their data were somewhat secure (24.0%) or not secure (23.5%).

Table 4.12

Security of data when teleworking

Security of data when teleworking	Frequency	Percentage
My data are not secure	47	23.5
My data are somewhat secure	48	24.0
My data are very secure	105	52.5
Total	**200**	**100.0**

Relatedly, the employees were asked who had the responsibility for the security of their client devices when teleworking (Table 4.13). It could be seen that the majority (85.5%) believed that the firm was responsible for the security of their client devices. A small proportion (13.5%) believed that the responsibility rested with themselves as they used their own devices.

Table 4.13

Responsibility for security of client devices

Responsibility for the security of client devices	Frequency	Percentage
My organisation	171	85.5
Third-party	2	1.0
Myself (I use my own devices and am responsible for their security)	27	13.5
Total	**200**	**100.0**

The employees were asked about the security measures implemented/enforced by the organisation during teleworking (Table 4.14). It was found that the more popular security measures utilised were “Requires a password/passcode and/or other authentication before accessing the organization’s resources” (91.0%), “Regular application of device manufacturer updates and patches to protect devices from known vulnerabilities” (89.0%), “Separate user account with limited privileges” (82.0%), "Remote access is logged" (76.5%), "Session locking (access is prevented after a period of inactivity, e.g., 15 minutes)" (75.5%), "Personal firewalls" (73.5%),"Restrict which applications may be installed through whitelisting or blacklisting" (67.5%), "Backup of data" (67.5%), "Use of virtual machines (VMs)" (64.5%), "Data encryption of stored data on both built-in storage and removable media" (62.0%), and "Data encryption of sensitive data on both built-in storage and removable media" (60.0%). Less popular measures, perhaps obviously, were "Antimalware programs" (27.5%), "Limited networking capabilities for mobile device" (45.0%), and "Physical securing of telework PCs/laptops (e.g., using cable locks)" (19.0%).

Table 4.14

Security measures implemented/enforced by organisation

Security measures implemented/enforced by organisation	**Yes (%)**	**No (%)**
Separate user account with limited privileges	164 (82.0)	36 (18.0)
Session locking (access is prevented after a period of inactivity, e.g., 15 minutes)	151 (75.5)	49 (24.5)
Physical securing of telework PCs/laptops (e.g., using cable locks)	38 (19.0)	162 (81.0)
Limited networking capabilities for mobile device	90 (45.0)	110 (55.0)
Antimalware programs	55 (27.5)	145 (72.5)
Personal firewalls	147 (73.5)	53 (26.5)
Regular application of device manufacturer updates and patches to protect devices from known vulnerabilities	178 (89.0)	22 (11.0)
Data encryption of stored data on both built-in storage and removable media	124 (62.0)	76 (38.0)
Data encryption of sensitive data on both built-in storage and removable media	120 (60.0)	80 (40.0)

Security measures implemented/enforced by organisation	Yes (%)	No (%)
Requires a password/passcode and/or other authentication before accessing the organization’s resources	182 (91.0)	18 (9.0)
Restrict which applications may be installed through whitelisting or blacklisting	135 (67.5)	65 (32.5)
Use of virtual machines (VMs)	129 (64.5)	71 (35.5)
Backup of data	135 (67.5)	65 (32.5)
Remote access is logged	153 (76.5)	47 (23.5)

Table 4.15 summarises the employees’ perceptions of their productivity at home. The majority (89.0%) believed that they were more productive at home.

Table 4.15
Productivity at home

Productivity at home	Frequency	Percentage
More productive at home	178	89.0
Less productive at home	22	11.0
Total	**200**	**100.0**

Table 4.16 summarises the employees’ perceptions regarding teleworking when the situation returned to normalcy after the pandemic. The majority (46.5%) indicated that they would like to continue teleworking and supported more telework. This was followed by a group (41.0%) who also indicate that they would like to continue to telework, but in a reduced frequency. The minority (12.5%) indicated that they would like to return to office on a full-time basis.

Table 4.16
Teleworking when things return to ‘normal’

Telework when things return to ‘normal’	Frequency	Percentage
Yes, more telework	93	46.5
Yes, less telework	82	41.0
No, I want to return to office	25	12.5

Telework when things return to 'normal'	Frequency	Percentage
Total	**200**	**100.0**

The employees used different forms of communication channels in teleworking. The most common were email, chat/instant messaging, and video (Table 4.17). The decrease in usage of phone calls could be clearly seen as only 6.5% of the participants used this while teleworking.

Table 4.17
Communication channels utilised

Communication channel		E-mail	Phone (e.g., calls on mobile/land line, WhatsApp call, Skype call)	Chat/Instant Messaging (e.g., Skype, Microsoft Teams, etc.)	Video (e.g., Zoom, Microsoft Teams, etc.)
Yes	Frequency	200	13	198	200
	Percentage	100	6.5	99	100
No	Frequency	0	187	2	0
	Percentage	0	93.5	1	0
Total	**Frequency**	**200**	**200**	**200**	**200**
	Percentage	**100**	**100**	**100**	**100**

Productivity while teleworking

The data obtained from the case study were also explored by means of descriptive analysis to ascertain the overall trends in the data. The employees' perceptions regarding their work features such as job role, job performance, work autonomy, and job complexity, were analysed and the mean and standard deviation was obtained in this regard (Table 4.18).

Overall, it could be seen that the employees were clear about their job role as the data indicated that they agreed that they were clear about what is expected of them at work (4.325±0.956); they were clear what their duties and responsibilities were (4.340±0.905); and they understood how their work fits into the overall aims of the organization (4.345±0.944). On the other hand, they seemed to have mixed opinions regarding how to go about getting their job done (3.190±0.921) and their clarity regarding the goals and objectives for their departments (3.035±0.893).

Regarding job performance, it could be seen that the employees agreed that they felt that they have been effectively fulfilling their roles and responsibilities when teleworking (4.415±0.852) and their overall performance is very good/outstanding when teleworking (4.265±0.959). The employees also signified that to a lower extent that their overall performance is good/above average when teleworking (3.600±1.003) or their overall performance is at least average when teleworking (3.525±1.065). In contrast, they disagreed their overall performance is poor/below average when teleworking (1.630±0.852). It could be inferred that the employees believed that teleworking had been beneficial to their performance on the job.

The employees' perceptions regarding their work autonomy during teleworking was a little varied. For instance, they agreed that they were allowed to plan how to do their work (4.370±0.852); they were allowed to use their personal initiative or judgment in carrying out the work (4.355±0.896); they were allowed to make decisions about what methods they use to complete their work (4.410±0.852); they have considerable opportunity for independence and freedom in how they do the work (4.285±0.937); and they were allowed to decide on their own how to go about doing their work (4.422±0.900). On the other hand, they seemed to have mixed feelings (neither agreeing nor disagreeing) regarding their being allowed to make their own decisions about how to schedule their work (3.425±0.905); being allowed to decide on the order in which things are done on the job (3.780±0.745); being allowed to make a lot of decisions on their own (3.790±0.944); and being given significant autonomy in making decisions (3.655±0.767).

Regarding the complexity of their work, the employees agreed that their job tasks were intricate and complex (4.345±0.959); required that they engage in a large amount of thinking (4.240±0.936); required them to keep track of more than one thing at a time (4.420±0.859); required the use of a number of skills (4.285±0.948); were highly specialized in terms of purpose, tasks, or activities (4.360±0.919); required very specialized knowledge and skills (4.375±0.894); and required a depth of knowledge and expertise (4.225±1.039). In contrast, they were less in agreement regarding whether their job involved a great deal of task variety (3.370±1.273); required that they only do one task or activity at a time (3.445±1.218); required them to monitor a great deal of information (3.375±0.823); and required them to analyse a lot of information (3.415±1.033).

Table 4.18

Work features

Work features	Mean	Std. Deviation
Job Role		
I am clear what is expected of me at work	4.325	0.956
I know how to go about getting my job done	3.190	0.921
I am clear what my duties and responsibilities are	4.340	0.905
I am clear about the goals and objectives for my department	3.035	0.893
I understand how my work fits into the overall aim of the organization	4.345	0.944
Job performance		
Overall, I feel I have been effectively fulfilling their roles and responsibilities when teleworking	4.415	0.852
My overall performance is very good/outstanding when teleworking	4.265	0.959
My overall performance is good/above average when teleworking	3.600	1.003
My overall performance is average when teleworking	3.525	1.065

Work features	Mean	Std. Deviation
My overall performance is poor/below average when teleworking	1.630	0.852
Work autonomy		
I can make my own decisions about how to schedule my work.	3.425	0.905
I am allowed to decide on the order in which things are done on the job.	3.780	0.745
I am allowed to plan how I do my work	4.370	0.852
I am allowed to use my personal initiative or judgment in carrying out the work	4.355	0.896
I am allowed to make a lot of decisions on my own	3.790	0.944
I am given significant autonomy in making decisions	3.655	0.767
I am allowed to make decisions about what methods I use to complete my work.	4.410	0.852
I have considerable opportunity for independence and freedom in how I do the work	4.285	0.937
I am allowed to decide on my own how to go about doing my work	4.422	0.900
Job complexity		
My job involves a great deal of task variety	3.370	1.273
My job requires that I only do one task or activity at a time	3.445	1.218
My job tasks are intricate and complex	4.345	0.959
My job requires me to monitor a great deal of information.	3.375	0.823
My job requires that I engage in a large amount of thinking.	4.240	0.936
My job requires me to keep track of more than one thing at a time.	4.420	0.859
My job requires me to analyse a lot of information.	3.415	1.033
My job requires the use of a number of skills.	4.285	0.948
My job is highly specialized in terms of purpose, tasks, or activities.	4.360	0.919
My job requires very specialized knowledge and skills.	4.375	0.894
My job requires a depth of knowledge and expertise.	4.225	1.039

The employees were also asked about their perceptions regarding aspects of their own productivity during teleworking (Table 4.19). Regarding their perceived productivity, the employees indicated that their productivity at work has improved while teleworking despite greater number of meetings and other communication (4.140±0.802); that they were more efficient in their work when teleworking (4.330±0.695); they were able to collaborate well with peers while teleworking (4.220±0.731); and were able to obtain guidance and feedback from their manager while teleworking (4.185±0.723). They also indicated that they were able to be productive in their work when teleworking (3.820±0.735).

As regards their productivity level, the employees strongly indicated that these had improved while teleworking. For example, it appeared that the majority agreed that their productivity was Hugely better (4.155±0.998) or Substantially better (4.385±0.855). Fewer employees agreed that their productivity was Better (3.755±1.020) or Same (3.625±1.387). Accordingly, the majority disagreed that their productivity had become Worse (1.725±0.940); Substantially worse (1.565±0.854); or Hugely worse (1.750±0.878).

The employees' perceptions regarding measurement of productivity by the organization revealed that they agreed that their organisation sets and communicates clear goals and deadlines in the same way as they do with workers in a physical workspace (4.240±0.958); has formed plans to increase their accountability (4.400±0.908); analyses important tasks and track progress on a time bound basis (4.455±0.813); evaluates quality and quantity instead of time worked (4.405±0.809); has shifted metrics from "hours spent" to "tasks accomplished and their quality" (4.500±0.814); and tracks their achievements (4.390±0.878).

Table 4.19

Productivity while teleworking

Productivity while teleworking	Mean	Std. Deviation
Perceived productivity		

Productivity while teleworking	Mean	Std. Deviation
My productivity at work has improved while teleworking despite greater number of meetings and other communication	4.140	0.802
I am more efficient in my work when teleworking	4.330	0.695
I am able to collaborate well with peers while teleworking	4.220	0.731
I am able to obtain guidance and feedback from my manager while teleworking	4.185	0.723
I am able to be productive in my work when teleworking	3.820	0.735
Productivity level		
Hugely better - I am 20+% more productive than I expected to be while teleworking	4.155	0.998
Substantially better - I am to 10% to 19% more productive than I expected to be while teleworking	4.385	0.855
Better - I am 1% to 9% more productive than I expected to be while teleworking	3.755	1.020
Same - I am at about the same level of productivity while teleworking	3.625	1.387
Worse - I am 1% to 9% less productive than I expected to be while teleworking	1.725	0.940
Substantially worse - I am to 10% to 19% less productive than I expected to be while teleworking	1.565	0.854
Hugely worse -- I am 20%+ less productive than I expected to be while teleworking	1.750	0.878
Organization measure of Productivity		
My organisation sets and communicates clear goals and deadlines in the same way as they do with workers in a physical workspace	4.240	0.958
My organisation has formed plans to increase my accountability	4.400	0.908
My organisation analyses important tasks and track progress on a time bound basis	4.455	0.813
My organisation evaluates quality and quantity instead of time worked	4.405	0.809
My organisation has shifted metrics from “hours spent” to “tasks accomplished and their quality”	4.500	0.814
My organisation tracks my achievements	4.390	0.878

VPN and teleworking

The employees were found to use different VPN solutions while teleworking (Table 4.20). The most popular options included ExpressVPN (16.0%), NordVPN (11.0%), and Hotspot (10.5%). However, it may be noted that the employees seemed open to use the different VPN solutions available in the market.

Table 4.20
VPN used

VPN used	**Frequency**	**Percentage**
ExpressVPN	32	16.0
NordVPN	22	11.0
Surfshark	12	6.0
Private Internet Access	15	7.5
IPVanish	16	8.0
Windscribe	13	6.5
ProtonVPN	12	6.0
CyberGhost VPN	14	7.0
PureVPN	15	7.5
VyprVPN	13	6.5
TunnelBear	15	7.5
Hotspot Shield	21	10.5
Total	**200**	**100.0**

The employees’ most popular reason for choosing a VPN solution was that it was provided to them by the organisation (43.5%). Other reasons included randomly encountering a solution while browsing (19.0%) or due to a recommendation from friends and family (17.5%) (Table 4.21).

Table 4.21
Reason for choosing VPN

Reason for choosing VPN	**Frequency**	**Percentage**
Actively researching on the Internet e.g., using a search engine	23	11.5
Recommendations from friends and family	35	17.5
I randomly encountered them while browsing the web, through advertisements	38	19.0
Recommendation websites e.g., CNET, TechRadar, Top10vpn	11	5.5
User review posts e.g., YouTube	6	3.0
My work provides me a VPN	87	43.5
Total	**200**	**100.0**

Since most of the employees used the VPN solution used by the organisation, they were not concerned about type of VPN subscription (Table 4.22).

Table 4.22
Type of VPN subscription

Type of VPN subscription	**Frequency**	**Percentage**
Free/trial version of a VPN service	56	28.0
Paid/premium version of a VPN service	57	28.5
Does not apply (Organisation or Custom VPN)	87	43.5
Total	**200**	**100.0**

The employees’ purpose of using a VPN product was mainly for file sharing (100%), to access region-specific content (98.5%), and to access work networks remotely (95%) (Table 4.23).

Table 4.23
Purpose of using a VPN product

Purpose of using a VPN product	Yes (%)	No (%)
To access work networks remotely	190 (95.0)	10 (50)
To protect myself from various threats/adversaries	84 (42.0)	116 (58.0)
For file sharing	200 (100.0)	0 (0.0)
To access region-specific content	197 (98.5)	3 (1.5)

Most of the employees (58.5%) used VPN all the time rather than occasionally or every week or every day (Table 4.23).

Table 4.25
Frequency of using VPN

Frequency of using VPN	Frequency	Percentage
Occasionally	28	14.0
Every week	17	8.5
Every day	38	19.0
All the time/Always on	117	58.5
Total	**200**	**100.0**

The employees were asked their opinion regarding different facets of VPN usage (Table 4.24). Regarding the link between VPN and productivity, the employees indicated that they agreed that VPN helps secure their connection to the organisation network (4.055±0.717); VPN helps with productivity in teleworking (3.820±0.762); and they do not have to worry about the security of their data (3.825±0.622).

The employees' knowledge of the VPN concept was strong in some areas. For instance, the majority seemed to be aware that it is a network that can be connected remotely (4.320±0.873) and it is an application for information privacy and security (4.495±0.821). On the other hand, they seemed to have slightly lower awareness that it was an application to encrypt internet connection (3.455±0.671) or that it was an application for digital anonymity (3.540±0.832). Similarly, they had lower awareness regarding its being an application for internet censorship circumvention (3.435±0.734) or that it was a tool to secure internet connection (3.825±0.683).

The employees also showed some awareness regarding VPN functioning. They were aware that it is a subscription-based model (3.840±1.000); uses a high-speed leased line (3.830±0.967); and with VPN, dial-up modems can be used to connect remote locations to the Internet (3.590±1.422).

The employees also were aware of VPN risks and advantages. For example, they were aware that Hackers and computer thieves can decrypt VPN connection (4.430±0.854); VPN applications require access rights to sensitive resources such as user accounts (4.305±0.892); VPN applications contain malware that affects the security of the operating system (4.455±0.819); VPN applications collect users' personal information and sell them to external partners (4.305±0.881); VPN applications track the location of the device by accessing the GPS of the user's device (3.360±0.851); VPN applications allow sharing the IP address given by the application with other users (4.460±0.807); VPN applications direct the browser to websites without your permission (4.440±0.824); and VPN applications steal network bandwidth and resell it (4.330±0.857). Similarly, as regards VPN Advantages, the employees were aware that VPNs eliminate geographical restrictions (4.460±0.826); Online privacy is safeguarded (4.420±0.829); My connection is protected from cyber criminals (4.515±0.709); Data transfer is encrypted (3.910±0.681); Regional leased lines or even cable networks can be used to connect to the internet (4.325±0.826); Cost saving (4.210±0.980); and Uses public networks to tunnel a private connection (4.330±0.903).

Table 4.24
Facets of VPN usage

Facets of VPN usage	Mean	Std. Deviation
VPN and Productivity		
VPN helps with productivity in teleworking	3.820	0.762
VPN helps secure my connection to the organisation network	4.055	0.717
I do not have to worry about the security of my data	3.825	0.622
Awareness of VPN Concept		
Network that can be connected remotely	4.320	0.873
Application to encrypt internet connection	3.455	0.671
Application for digital anonymity	3.540	0.832
Application for internet censorship circumvention	3.435	0.734
Tool to secure internet connection	3.825	0.683
Application for information privacy and security	4.495	0.821
VPN Functioning		
VPN is a subscription-based model	3.840	1.000
VPN uses a high-speed leased line	3.830	0.967
With VPN, dial-up modems can be used to connect remote locations to the Internet	3.590	1.422
VPN Risks		
Hackers and computer thieves can decrypt VPN connection	4.430	0.854
VPN applications require access rights to sensitive resources such as user accounts	4.305	0.892
VPN applications contain malware that affects the security of the operating system	4.455	0.819
VPN applications collect users’ personal information and sell them to external partners	4.305	0.881

Facets of VPN usage	Mean	Std. Deviation
VPN applications track the location of the device by accessing the GPS of the user’s device	3.360	0.851
VPN applications allow sharing the IP address given by the application with other users	4.460	0.807
VPN applications direct the browser to websites without your permission	4.440	0.824
VPN applications steal network bandwidth and resell it	4.330	0.857
VPN Advantages		
VPNs eliminate geographical restrictions	4.460	0.826
Online privacy is safeguarded	4.420	0.829
My connection is protected from cyber criminals.	4.515	0.709
Data transfer is encrypted.	3.910	0.681
Regional leased lines or even cable networks can be used to connect to the internet.	4.325	0.826
Cost saving.	4.210	0.980
Uses public networks to tunnel a private connection	4.330	0.903

Reliability Analysis

The reliability of the questionnaire was tested using Cronbach’s alpha (Table 4.25). It was found that the alpha values ranged between 0.609 for Awareness of VPN Concept and Work autonomy, and 0.896 for Perceived productivity. While a general rule of thumb applicable to alpha values is “ = .9 – Excellent, = .8 – Good, = .7 – Acceptable, = .6 – Questionable, = .5 – Poor, and = .5 – Unacceptable,” there is no fixed interpretation as regards what is an acceptable value for alpha (George and Mallery, 2019, p. 244). In the present study, though only five of the twelve variables had alpha values greater than 0.7, it could be inferred that the scale had moderate to excellent reliability.

Table 4.25

Reliability Analysis

Factors	**Sub factors**	**Variables**	**Cronbach's Alpha**	**N of Items**
Productivity while teleworking	Work features	Job Role	0.649	2
		Job performance	0.669	5
		Work autonomy	0.609	6
		Job complexity	0.727	11
	Productivity	Perceived productivity	0.896	5
		Productivity level	0.717	7
		Organization measure of Productivity	0.662	6
Facets of VPN usage		VPN and Productivity	0.861	3
		Awareness of VPN Concept	0.609	5
		VPN Functioning	0.825	3
		VPN Risks	0.671	8
		VPN Advantages	0.646	7

Validity Testing – Exploratory Factor Analysis

The sufficiency of the different scales utilised to measure the variables of the study, i.e., to assess whether the phenomenon under consideration could be completely characterised by the study’s hypotheses and outcomes, was tested by carrying out Exploratory Factor Analysis (EFA) utilising Varimax rotation. The most frequent use of EFA is to identify a “small number of factors that may be used to represent relationships among sets of interrelated variables” (George and Mallery, 2019, p. 258). The influence of one item on another was determined by its factor loading value. Values approaching 1 were considered to signify robust influence of a factor while values approaching 0 were considered to signify weak influence. In addition, adequate validity was considered to be signified by factor loading values >0.40 with Eigen value=1.

Two tests, Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO) and Bartlett's Test of sphericity, were first performed to assess the fitness of performing EFA on the data for the different scales (Bartlett, 1950; Kaiser, 1974; Cerny and Kaiser, 1977). The KMO test is a “measure of whether your distribution of values is adequate for conducting factor analysis.” Levels as are designated as follows: “A measure > .9 is marvelous, > .8 is meritorious, > .7 is middling, > .6 is mediocre, > .5 is miserable, and < .5 is unacceptable.” Bartlett’s test, on the other hand, is “a measure of the multivariate normality” of the set of distributions. Moreover, it assesses whether or not the correlation matrix is an identity matrix. A significance value < .05 indicates that the data are nearly multivariate normal and thus suitable for factor analysis (George and Mallery, 2019, p. 268).

Work features

KMO and Bartlett's Test of sphericity were performed to assess the suitability of performing EFA on the data for the work features scale (Table 4.26). The KMO value was found to be 0.646 with the Bartlett's Test of sphericity significant at 0.000, confirming the adequacy of sampling (Kaiser, 1974; Cerny and Kaiser, 1977).

Table 4.26
KMO and Bartlett's of work features scale

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.646
Bartlett's Test of Sphericity	Approx. Chi-Square	1174.956
	df	153
	Sig.	0.000

Eighteen factors were extracted with Eigenvalue >1 that explained 100% of the variance in the data (Table 4.27). Job role was found to be the most important variable as it explained 18.659% of the variance in the observed table. This was followed by Job Performance which explained 15.751% of the variance.

Table 4.27
Factors of work features scale

Factor	**Factor loadings**	**% of Variance**	**Cumulative %**
Job Role		**18.659**	**18.659**
I know how to go about getting my job done	0.843		
I am clear about the goals and objectives for my department	0.821		
I understand how my work fits into the overall aim of the organization	0.645		
Job performance		**15.751**	**34.409**
My overall performance is very good/outstanding when teleworking	0.632		
My overall performance is average when teleworking	0.622		
Overall, I feel I have been effectively fulfilling their roles and responsibilities when teleworking	0.615		
Work autonomy		**9.840**	**44.249**
I can make my own decisions about how to schedule my work.	0.887		
I am allowed to make a lot of decisions on my own	0.788		
I am allowed to decide on the order in which things are done on the job.	0.677		
I have considerable opportunity for independence and freedom in how I do the work	0.653		
I am given significant autonomy in making decisions	0.627		
Job complexity		**7.898**	**52.147**
My job tasks are intricate and complex	0.725		
My job requires me to analyse a lot of information.	0.684		

Factor	Factor loadings	% of Variance	Cumulative %
My job requires that I engage in a large amount of thinking.	0.652		
My job is highly specialized in terms of purpose, tasks, or activities.	0.613		
My job requires very specialized knowledge and skills.	0.602		
My job requires the use of a number of skills.	0.598		
My job requires me to keep track of more than one thing at a time.	0.558		

Productivity

KMO and Bartlett's Test of sphericity were performed to assess the suitability of performing EFA on the data for the work features scale (Table 4.28). The KMO value was found to be 0.755 with the Bartlett's Test of sphericity significant at 0.000, confirming the adequacy of sampling (Kaiser, 1974; Cerny and Kaiser, 1977).

Table 4.28
KMO and Bartlett's of productivity scale

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.755
Bartlett's Test of Sphericity	Approx. Chi-Square	1073.439
	df	55
	Sig.	0.000

Eleven factors were extracted with Eigenvalue >1 that explained 100% of the variance in the data (Table 4.29). Perceived productivity was found to be the most important variable as it explained 32.956% of the variance in the observed table. This was followed by Productivity level which explained 19.051% of the variance.

Table 4.29
Factors of productivity scale

		% of Varianc e	**Cumulativ e %**
Perceived productivity		**32.956**	**32.956**
I am more efficient in my work when teleworking	0.938		
I am able to collaborate well with peers while teleworking	0.958		
I am able to obtain guidance and feedback from my manager while teleworking	0.861		
My productivity at work has improved while teleworking despite greater number of meetings and other communication	0.794		
I am able to be productive in my work when teleworking	0.657		
Productivity level		**19.051**	**52.007**
Substantially better - I am to 10% to 19% more productive than I expected to be while teleworking	0.796		
Better - I am 1% to 9% more productive than I expected to be while teleworking	0.687		
Substantially worse - I am to 10% to 19% less productive than I expected to be while teleworking	0.751		
Hugely worse -- I am 20%+ less productive than I expected to be while teleworking	0.532		
Organization measure of Productivity		**12.647**	**64.654**
My organisation analyses important tasks and track progress on a time bound basis	0.859		
My organisation tracks my achievements	0.709		

VPN Usage

KMO and Bartlett's Test of sphericity were performed to assess the suitability of performing EFA on the data for the facets of VPN usage scale (Table 4.30). The KMO value was found to be 0.755 with the Bartlett's Test of sphericity significant at 0.000, confirming the adequacy of sampling (Kaiser, 1974; Cerny and Kaiser, 1977).

Table 4.30
KMO and Bartlett's of facets of VPN usage scale

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.687
Bartlett's Test of Sphericity	Approx. Chi-Square	1385.144
	df	171
	Sig.	0.000

Nineteen factors were extracted with Eigenvalue >1 that explained 100% of the variance in the data (Table 4.31). VPN Advantages was found to be the most important variable as it explained 18.485% of the variance in the observed table. This was followed by Awareness of VPN Concept which explained 14.937% of the variance.

Table 4.31
Factors of facets of VPN usage scale

Factors	**Factor loadings**	**% of Variance**	**Cumulative %**
VPN Advantages		**18.485**	**18.485**
Online privacy is safeguarded	0.661		
VPNs eliminate geographical restrictions	0.647		
Regional leased lines or even cable networks can be used to connect to the internet.	0.640		
My connection is protected from cybercriminals.	0.615		
Cost saving	0.599		

Factors	**Factor loadings**	**% of Variance**	**Cumulative %**
Uses public networks to tunnel a private connection	0.551		
Awareness of VPN Concept		**14.937**	**33.422**
Application to encrypt internet connection	0.841		
Application for digital anonymity	0.733		
Application for internet censorship circumvention	0.522		
VPN Functioning		**12.238**	**45.660**
VPN uses a high-speed leased line	0.909		
With VPN, dial-up modems can be used to connect remote locations to the Internet	0.900		
VPN is a subscription-based model	0.783		
VPN Risks		**8.498**	**54.158**
VPN applications require access rights to sensitive resources such as user accounts	0.711		
VPN applications contain malware that affects the security of the operating system	0.607		
VPN applications collect users' personal information and sell them to external partners	0.695		
VPN applications track the location of the device by accessing the GPS of the user's device	0.649		
VPN and Productivity		**6.511**	**60.669**

Factors	Factor loadings	% of Variance	Cumulative %
VPN helps with productivity in teleworking	0.909		
VPN helps secure my connection to the organisation network	0.890		
I do not have to worry about the security of my data	0.657		

Influence of participant demographics on work features

The study investigated if employees' perceptions regarding different aspects of their work features were significantly (p<0.05) affected by their demographic details. In this regard, their perceptions regarding Job Role were found to be influenced by Gender (F/t = 2.823). On the other hand, their perceptions regarding Job Performance were found to be influenced by Nature of employment (F/t = 3.529). Their perceptions regarding Work autonomy were found to be influenced by their Age (F/t=3.700), Educational qualification (F/t=3.404) and their Work experience (F/t=3.220). Finally, their perceptions regarding their Job complexity were found to be significantly influenced by Gender (F/t = 2.216) and Work experience (F/t = 3.370) (Table 4.32).

Table 4.32
Influence of demographics on Employees' perceptions of work features

	Job Role		Job performance		Work autonomy		Job complexity	
Gender								
Male	3.929±0.494	2.823 (0.005)	3.447±0.458	-1.515 (0.131)	4.037±0.388	-0.700 (0.485)	4.053±0.450	2.216 (0.028)
Female	3.733±0.477		3.543±0.433		4.079±0.434		3.896±0.521	
Age (years)								
21-30 years	3.853±0.553	0.053 (0.984)	3.489±0.408	0.102 (0.959)	3.980±0.376	3.700 (0.013)	4.04±0.435	1.191 (0.314)
31-40 years	3.855±0.482		3.495±0.456		4.040±0.418		3.994±0.482	
41-50 years	3.826±0.467		3.484±0.521		4.065±0.337		3.988±0.48	
51-60 years	3.813±0.515		3.427±0.392		4.370±0.452		3.77±0.646	
Educational qualification								
Graduate	3.846±0.509	0.323 (0.809)	3.479±0.458	0.394 (0.758)	4.068±0.409	3.404 (0.019)	3.992±0.490	0.678 (0.566)
Masters	3.909±0.441		3.600±0.390		4.000±0.243		4.033±0.391	
Doctorate	3.950±0.475		3.575±0.446		4.319±0.454		4.091±0.370	
Diploma	3.757±0.409		3.443±0.401		3.786±0.353		3.825±0.574	
Nature of employment								
Full time	3.844±0.493	1.399 (0.244)	3.520±0.433	3.529 (0.016)	3.999±0.479	1.481 (0.221)	4.168±0.485	0.711 (0.546)
Part-time	3.980±0.527		3.260±0.520		3.909±0.506		4.086±0.492	
Contractor	3.767±0.344		3.600±0.420		4.167±0.211		4.242±0.179	
Intern	3.450±0.526		3.050±0.342		3.568±0.857		3.864±0.848	
Work experience (years)								
<5	3.884±0.434	1.817 (0.127)	3.501±0.420	0.179 (0.949)	4.029±0.399	3.220 (0.014)	4.047±0.400	3.370 (0.011)
>5-10	3.872±0.555		3.497±0.431		4.142±0.435		4.005±0.497	
>10-20	3.681±0.490		3.490±0.476		3.896±0.346		3.760±0.612	
>20-30	3.900±0.429		3.450±0.518		4.130±0.431		4.121±0.379	
>30	4.086±0.662		3.371±0.571		4.286±0.201		4.143±0.267	

Influence of participant demographics on productivity

In addition, the study investigated if employees' perceptions regarding different aspects of their productivity were significantly ($p<0.05$) affected by their demographic details. In this regard, it was found that only their perceptions regarding Perceived productivity were influenced by Nature of employment (F/t = 4.58) and Work experience (F/t=2.489). It could be inferred hence, that Nature of employment and Work experience have a higher impact on the productivity of an employee than their gender, age, or educational qualification (Table 4.33).

Table 4.33

Influence of demographics on Employees' perceptions of productivity

	Perceived productivity		**Productivity level**		**Organization measure of productivity**	
Gender						
Male	4.100±0.633	-1.053 (0.294)	3.021±0.362	1.215 (0.226)	4.431±0.51	1.018 (0.310)
Female	4.193±0.602		2.957±0.366		4.353±0.551	
Age (years)						
21-30 years	4.147±0.626	0.359 (0.782)	3.019±0.316	0.150 (0.930)	4.489±0.447	0.654 (0.581)
31-40 years	4.105±0.619		2.995±0.344		4.37±0.560	
41-50 years	4.232±0.645		2.963±0.402		4.349±0.454	
51-60 years	4.173±0.604		2.981±0.556		4.433±0.654	
Educational qualification						
Graduate	4.150±0.608	1.948 (0.123)	2.982±0.384	0.624 (0.600)	4.387±0.560	0.767 (0.514)
Masters	3.891±0.589		3.065±0.309		4.545±0.326	
Doctorate	4.525±0.337		2.964±0.226		4.583±0.236	
Diploma	3.986±0.821		3.102±0.181		4.310±0.306	
Nature of employment						
Full time	4.182±0.601	4.58 (0.004)	3.005±0.370	0.452 (0.716)	4.388±0.540	1.217 (0.305)
Part-time	3.830±0.647		2.929±0.339		4.458±0.436	
Contractor	3.600±0.693		3.000±0.286		4.694±0.125	
Intern	4.650±0.191		2.857±0.387		4.083±0.687	
Work experience (years)						
<5	3.983±0.656	2.489 (0.045)	3.029±0.361	0.495 (0.739)	4.43±0.476	0.892 (0.47)
>5-10	4.262±0.539		2.956±0.389		4.451±0.551	
>10-20	4.148±0.68		2.976±0.390		4.266±0.483	
>20-30	4.158±0.563		2.988±0.295		4.424±0.693	
>30	4.543±0.36		3.102±0.257		4.357±0.413	

Influence of participant demographics on facets of VPN usage

Moreover, the study investigated if employees’ perceptions regarding different facets of their VPN usage were significantly ($p<0.05$) affected by their demographic details (Table 4.34). In contrast to the previous variables, it could be found that the perceptions of the variables were significantly impacted by many demographic variables in this regard. For instance, it was found that their perceptions regarding VPN and productivity were influenced by Gender (F/t = -2.277), Educational qualification (F/t = 5.25), Nature of employment (F/t = 4.366) and Work experience (F/t=4.054). Similarly, their perceptions regarding their Awareness of VPN concept were influenced by Age (F/t = 3.06), Educational qualification (F/t = 3.192), Nature of employment (F/t = 3.511) and Work experience (F/t=2.832). Their perceptions regarding VPN Functioning were influenced by Age (F/t = 4.114) and their perceptions regarding VPN Risks were influenced by their Gender (F/t = 2.26). Finally, their perceptions regarding VPN Advantages were influenced by their Educational qualification (F/t = 2.73) and their Work experience (F/t = 2.452).

Table 4.34

Influence of demographics on Employees' perceptions of facets of VPN usage

	VPN and Productivity		**Awareness of VPN Concept**		**VPN Functioning**		**VPN Risks**		**VPN Advantages**	
Gender										
Male	3.816±0.622	-2.277 (0.024)	3.833±0.441	-0.449 (0.654)	3.862±0.983	1.839 (0.068)	4.324±0.444	2.26 (0.025)	4.365±0.464	1.946 (0.053)
Female	4.016±0.605		3.861±0.425		3.603±0.982		4.173±0.485		4.235±0.467	
Age (years)										
21-30 years	3.867±0.613	0.443 (0.722)	3.874±0.393	3.06 (0.029)	3.83±1.002	4.114 (0.007)	4.364±0.445	1.189 (0.315)	4.371±0.432	0.387 (0.762)
31-40 years	3.878±0.623		3.813±0.444		3.813±0.956		4.229±0.479		4.292±0.506	
41-50 years	3.957±0.648		3.769±0.447		3.839±0.954		4.274±0.353		4.272±0.396	
51-60 years	4.044±0.615		4.144±0.344		2.911±0.955		4.15±0.622		4.333±0.451	
Educational qualification										
Graduate	3.93±0.611	5.25 (0.002)	3.858±0.43	3.192 (0.025)	3.768±0.972	0.209 (0.89)	4.252±0.488	1.64 (0.182)	4.317±0.475	2.73 (0.045)
Masters	3.727±0.467		3.788±0.409		3.788±1.067		4.534±0.186		4.403±0.277	
Doctorate	4.375±0.452		4.125±0.365		3.5±1.357		4.281±0.352		4.554±0.345	
Diploma	3.405±0.656		3.571±0.417		3.69±0.991		4.134±0.358		4.02±0.468	
Nature of employment										
Full time	3.933±0.612	4.366 (0.005)	3.873±0.417	3.511 (0.016)	3.725±1.017	0.35 (0.789)	4.271±0.46	1.201 (0.311)	4.324±0.456	1.241 (0.296)
Part-time	3.6±0.558		3.708±0.489		3.9±0.758		4.206±0.494		4.136±0.543	
Contractor	3.5±0.691		3.389±0.417		3.833±1.07		4.396±0.146		4.381±0.309	
Intern	4.583±0.419		4.042±0.479		4.083±0.833		3.875±0.835		4.5±0.742	
Work experience (years)										
<5	3.734±0.582	4.054 (0.004)	3.78±0.407	2.832 (0.026)	3.773±0.933	0.521 (0.72)	4.321±0.411	1.827 (0.125)	4.306±0.44	2.452 (0.047)
>5-10	4.029±0.57		3.925±0.425		3.644±1.054		4.183±0.491		4.33±0.472	

	VPN and Productivity		**Awareness of VPN Concept**		**VPN Functioning**		**VPN Risks**		**VPN Advantages**	
>10-20	3.841±0.692		3.73±0.457		3.905±0.964		4.167±0.525		4.163±0.495	
>20-30	3.986±0.594		3.958±0.443		3.764±1.127		4.406±0.382		4.429±0.46	
>30	4.524±0.539		4.119±0.343		3.524±0.663		4.375±0.573		4.653±0.358	

Impact of work features on productivity of teleworking employees

The impact of work features on the productivity of teleworking employees was analysed using Multivariate Analysis of Variance (MANOVA). The following hypothesis was framed to evaluate the relationship between work features and the productivity of teleworking employees:

H1: Work features have a positive impact on productivity of teleworking employees

Work features of teleworking employees was considered as the independent variable and productivity of teleworking employees was considered as the dependent variable. The results of MANOVA are provided in Tables 4.35 and 4.37.

One-way MANOVA showed a significant impact of Job Role (Wilks' lambda = 0.905, F = 6.943, $p < 0.001$), Work autonomy (Wilks' lambda = 0.913, F = 6.101, $p < 0.001$), and Job complexity (Wilks' lambda = 0.856, F = 10.802, $p < 0.001$) on productivity of teleworking employees (Table 4.35).

Table 4.35

Multivariate Test for impact of work features on productivity of teleworking employees

Effect	Wilks' Lambda Value	F	df	Sig.
Job role	0.905	6.943	3, 193	0.010
Job performance	0.989	0.744	3, 193	0.527
Work autonomy	0.913	6.101	3, 193	0.001
Job complexity	0.856	10.802	3, 193	0.000

The Test of Between-subject effects showed that Job role (F = 16.844, $p < 0.001$, R^2 = 12.8%) and work autonomy (F = 15.976, $p < 0.001$, R^2 = 12.8%) had a significant impact on Perceived productivity of employees. In addition, job complexity had a significant impact on productivity level (F = 5.579, $p < 0.001$, R^2 = 2.4%) and organization measure of productivity (F = 22.146, $p < 0.001$, R^2 = 20.3%) (Table 4.36).

Consequently, hypothesis H1, *Work features have a positive impact on productivity of teleworking employees*, can be partially accepted.

Table 4.36

Test Between Subject-Effect work features on productivity of teleworking employees

Work feature	Productivity	Type III Sum of Squares	df	Mean Square	F	Sig.
Job role	Perceived productivity	5.652	1	5.652	16.844	0.000
	Productivity level	0.044	1	0.044	0.337	0.562
	Organization measure of Productivity	0.799	1	0.799	3.605	0.059
Job performance	Perceived productivity	0.023	1	0.023	0.068	0.795
	Productivity level	0.004	1	0.004	0.029	0.866
	Organization measure of Productivity	0.458	1	0.458	2.066	0.152
Work autonomy	Perceived productivity	5.361	1	5.361	15.976	0.000
	Productivity level	0.008	1	0.008	0.065	0.799
	Organization measure of Productivity	0.545	1	0.545	2.457	0.119
Job complexity	Perceived productivity	0.540	1	0.540	1.608	0.206
	Productivity level	0.723	1	0.723	5.579	0.019
	Organization measure of Productivity	4.909	1	4.909	22.146	0.000
R Squared = .146 (Adjusted R Squared = .128)						
R Squared = .043 (Adjusted R Squared = .024)						
R Squared = .219 (Adjusted R Squared = .203)						

Impact of facets of VPN usage on productivity of teleworking employees

The impact of facets of VPN usage on the productivity of teleworking employees was analysed using Multivariate Analysis of Variance (MANOVA). The following hypothesis was framed to evaluate the relationship between facets of VPN usage and the productivity of teleworking employees:

H2: Facets of VPN usage have a positive impact on productivity of teleworking employees

Facets of VPN usage was considered as the independent variable and productivity of teleworking employees was considered as the dependent variable. The results of

MANOVA are provided in Tables 4.37 and 4.38. One-way MANOVA showed a significant impact of VPN and productivity (Wilks' lambda = 0.613, F = 40.466, p < 0.001), VPN risks (Wilks' lambda = 0.935, F = 4.372, p < 0.001), and VPN advantages (Wilks' lambda = 0.935, F = 4.372, p < 0.001) on productivity of teleworking employees (Table 4.37).

Table 4.37

Multivariate Test for impact of facets of VPN on productivity of teleworking employees

Effect	Wilks' Lambda Value	F	df	Sig.
VPN and productivity	0.613	40.466	3, 192	0.000
Awareness of VPN concept	0.992	.073	3, 192	0.682
VPN functioning	0.987	.813	3, 192	0.488
VPN risks	0.841	12.080	3, 192	0.000
VPN advantages	0.935	4.372^b	3, 192	0.005

The Test of Between-subject effects showed that VPN and productivity (F = 117.606, p < 0.001, R^2 = 42.9%) had a significant impact on Perceived productivity of employees. In addition, VPN Risks had a significant impact on productivity level (F = 23.415, p < 0.001, R^2 = 21.2%) and organization measure of productivity (F = 23.415, p < 0.001, R^2 = 23.5%). VPN Advantages had a significant impact on organization measure of productivity (F = 12.891, p < 0.001, R^2 = 23.5%) (Table 4.38). Thus, hypothesis H2, *Facets of VPN usage have a positive impact on productivity of teleworking employees,* can also be partially accepted.

Table 4.38

Test Between Subject-Effect of facets of VPN on productivity of teleworking employees

Facets of VPN	Productivity	Type III Sum of Squares	df	Mean Square	F	Sig.
VPN and productivity	Perceived productivity	25.825	1	25.825	117.606	0.000
	Productivity level	0.146	1	0.146	1.132	0.289
	Organization measure of Productivity	0.134	1	0.134	0.632	0.428

Facets of VPN	Productivity	Type III Sum of Squares	df	Mean Square	F	Sig.
Awareness of VPN concept	Perceived productivity	0.031	1	0.031	0.141	0.708
	Productivity level	0.163	1	0.163	1.264	0.262
	Organization measure of Productivity	0.007	1	0.007	0.031	0.861
VPN Functioning	Perceived productivity	0.148	1	0.148	0.674	0.413
	Productivity level	0.002	1	0.002	0.016	0.898
	Organization measure of Productivity	0.327	1	0.327	1.537	0.217
VPN Risks	Perceived productivity	0.001	1	0.001	0.006	0.938
	Productivity level	1.114	1	1.114	8.640	0.004
	Organization measure of Productivity	4.983	1	4.983	23.415	0.000
VPN Advantages	Perceived productivity	0.003	1	0.003	0.014	0.907
	Productivity level	0.001	1	0.001	0.005	0.942
	Organization measure of Productivity	2.743	1	2.743	12.891	0.000
a. R Squared = .444 (Adjusted R Squared = .429)						
b. R Squared = .232 (Adjusted R Squared = .212)						
c. R Squared = .254 (Adjusted R Squared = .235)						

Impact of work features on facets of VPN usage

The impact of work features on facets of VPN usage was analysed using Multivariate Analysis of Variance (MANOVA). The following hypothesis was framed to evaluate the relationship between work features and facets of VPN usage:

H3: Work features have a positive impact on facets of VPN usage

Work features was considered as the independent variable and Facets of VPN usage was considered as the dependent variable. The results of MANOVA are provided in Tables 4.39 and 4.40. One-way MANOVA showed a significant impact of Job role (Wilks' lambda = 0.815, F = 8.668, p < 0.001), Work autonomy (Wilks' lambda = 0.682, F = 17.811, p < 0.001), and Job complexity (Wilks' lambda = 0.888, F = 4.801, p < 0.001) on facets of VPN usage of teleworking employees (Table 4.39).

Table 4.39

Multivariate Test for impact of work features on facets of VPN usage

Effect	Wilks' Lambda Value	F	df	Sig.
Job role	0.815	8.668	5, 191	0.000
Job performance	0.988	0.482	5, 191	0.789
Work autonomy	0.682	17.811	5, 191	0.000
Job complexity	0.888	4.801	5, 191	0.000

The Test of Between-subject effects showed that Job Role had a significant impact on VPN and Productivity (F = 36.734, p < 0.001, R^2 = 35.3%) and VPN Risks (F = 6.040, p < 0.05, R^2 = 17.3%). Work autonomy had a significant impact on VPN and Productivity (F 77.908, p < 0.001, R^2 = 35.3%) and Awareness of VPN concept (F = 30.835, p < 0.001, R^2 = 15.5%). Job complexity had a significant impact on VPN Risks (F = 21.179, p < 0.001, R^2 = 17.3%) and VPN Advantages (F = 9.823, p < 0.001, R^2 = 12.6%) (Table 4.40). Thus, hypothesis H3, *Work features have a positive impact on facets of VPN usage*, can be partially accepted.

Table 4.40

Test Between Subject-Effect of facets of work features on facets of VPN usage

Work feature	Facets of VPN usage	Type III Sum of Squares	df	Mean Square	F	Sig.
Job role	VPN and Productivity	9.182	1	9.182	36.734	0.000
	Awareness of VPN Concept	0.012	1	0.012	0.077	0.781
	VPN Functioning	0.011	1	0.011	0.012	0.914
	VPN Risks	1.090	1	1.090	6.040	0.015
	VPN Advantages	0.562	1	0.562	2.934	0.088

Work feature	Facets of VPN usage	Type III Sum of Squares	df	Mean Square	F	Sig.
Job performance	VPN and Productivity	0.020	1	0.020	0.081	0.776
	Awareness of VPN Concept	0.003	1	0.003	0.016	0.899
	VPN Functioning	0.591	1	0.591	0.599	0.440
	VPN Risks	0.102	1	0.102	0.563	0.454
	VPN Advantages	0.087	1	0.087	0.453	0.502
Work autonomy	VPN and Productivity	19.474	1	19.474	77.908	0.000
	Awareness of VPN Concept	4.893	1	4.893	30.835	0.000
	VPN Functioning	1.286	1	1.286	1.302	0.255
	VPN Risks	0.152	1	0.152	0.841	0.360
	VPN Advantages	0.671	1	0.671	3.503	0.063
Job complexity	VPN and Productivity	0.002	1	0.002	0.006	0.937
	Awareness of VPN Concept	0.186	1	0.186	1.170	0.281
	VPN Functioning	0.658	1	0.658	0.666	0.415
	VPN Risks	3.821	1	3.821	21.179	0.000
	VPN Advantages	1.883	1	1.883	9.823	0.002
a. R Squared = .366 (Adjusted R Squared = .353)						
b. R Squared = .172 (Adjusted R Squared = .155)						
c. R Squared = .010 (Adjusted R Squared = -.010)						
d. R Squared = .189 (Adjusted R Squared = .173)						
e. R Squared = .144 (Adjusted R Squared = .126)						

4.4 Findings from the interviews

The population for the qualitative segment of the study consisted of six different stakeholders. Three persons each were included from the management and IT teams. The persons from the management team were a Director/VP in Human Resources and two Delivery Managers. The persons from the IT team were Head of IT Infrastructure, a Manager of IT Infrastructure, and Head/Manager of Information Security. Table 4.41 summarises the details of the participants.

Table 4.41:
Interviewee details

Demographic details	**Gender**	**Educational qualification**	**Overall work experience**	**Current role**	**Responsibilities**
Mgt_1	Female	Masters in Business Administration	20 years	VP in Human Resources	planning, leading, directing, developing, and coordinating the policies, activities, and staff of the HR department; involved in ensuring legal compliance and implementation of the mission and talent strategy of the organisation.
Mgt_2	Female	B.E. Computer Science and Engineering	25 years	Delivery Manager (Manufacturing client)	Overseeing the program and project teams for a certain client in the Manufacturing line of business; tasks include monitoring progress, tracking performance indicators, and managing budgets
Mgt_3	Male	B.E. Electrical and Electronics Engineering	15 years	Delivery Manager (Banking client)	Planning, supervising, and coordinating programs and projects for a client in the Banking and Financial Services line of business; tasks include planning technical deliverables, ensuring compliance with client security standards, keeping track of budget, etc.
IT_1	Male	Masters in IT	>20 years	Head of IT Infrastructure	Responsible for the implementation and operations of all technology infrastructure which includes data centre, network and server services, telephony, service monitoring, user support/help desk, workstation management, servers, storage and related software

Demographic details	**Gender**	**Educational qualification**	**Overall work experience**	**Current role**	**Responsibilities**
IT_2	Male	Bachelors in Computer Science and Engineering	10 years	Manager of IT Infrastructure	Responsible for workstation management, servers, storage and related software
IT_3	Male	Bachelors in Computer Science and Engineering	10 years	Head/Manager of Information Security	Responsible for protecting the sensitive data. We do this by detecting and responding to incidents as well as planning preventative measures, such as encryption. Security teams manage network security (LAN and WAN), end-point security (laptops, cell phones, tablets), and internet security (documents or other files downloaded from the internet)

These six persons were approached due to their direct influence on teleworking policy and interaction with teleworking employees. Moreover, they were included in the study due to their availability and readiness to participate in the study.

Two interview guides were developed and utilised in the study to collect data from the participants. One was for the management team and the other for the IT team. Both interview guides were semi-structured to permit rich dialogue between the researcher and the participants (Merriam and Tisdell, 2016).

The analysis of the qualitative data revealed three main themes, each of which is supported by sub-themes and representative quotes. The themes are summarised in Table 4.42.

Table 4.42:
Emergent Themes and Sub-themes

Theme	**Sub-theme**
Facets of telework in the case organisation	1. Teleworking prior to the pandemic 2. Roles/jobs better suited for teleworking 3. Organisational support for telework 4. Tools used during teleworking
Impacts of telework	1. Productivity in teleworking 2. Support for productivity 3. Changes to teleworking policy 4. Managing files and data 5. Cybersecurity risks and threats 6. Security and teleworking
Facets of VPN usage	1. VPN features 2. VPN and teleworking 3. Benefits and risks of VPN usage 4. Factors to be considered prior to continued VPN use

4.4.1 Theme 1: Facets of telework in the case organisation

The first theme was related to facets of telework in the case organisation. Four sub-themes could be identified in relationship with the first theme namely, Teleworking prior to the pandemic; Roles/jobs better suited for teleworking; Organisational support for telework; and Tools used during teleworking.

Sub-theme 1: Teleworking prior to the pandemic

The COVID pandemic caused considerable changes to the way organisations worked as most of them had to change their operations to permit teleworking of all employees regardless of job role or grade. It appeared that the case study organisation had already allowed teleworking prior to the pandemic and had a policy to this effect. However, the eligibility for teleworking seemed to be dependent on role, grade, or manager approval. In addition, there was a restriction regarding the number of days per month that an employee could telework. IT_1 described the policy as follows:

> *"We had a policy for teleworking where an employee could work up to seven days per month based on the kind of project with exceptions permitted at manager and HR discretion.*

Mgt_1 added more detail regarding the eligibility criteria:

> *"We did have a policy which stipulated the grades which were eligible for telework, number of hours of telework allowed per month, approvals, usage of devices, exception cases, etc."*

Some more insights were provided by Mgt_2 who stated in her narrative that:

> *"Yes, the company implemented a teleworking policy before the pandemic. Delivery Managers were allowed to permit telework based on certain criteria such as, client requirements and role. In our unit, we followed the organisation*

> *policy and permitted telework a few days (40-50 hours per month) for employees who were eligible for laptops. Typically, team leads and above."*

The overall situation was summarised as follows by IT_1:

> *"Yes, teleworking was allowed before the pandemic. But not all employees were allowed. It was based on role/grade and manager's approval was necessary for exceptions."*

The narratives of the other IT executives (IT_2 and IT_3) corroborated this description as they affirmed that teleworking was permitted for some employees based on role/grade with manager's approval being required for any exceptions.

The perspectives of the Management team also corresponded with this description of the situation in the case organisation prior to the pandemic. For instance, Mgt_1 mentioned that the criteria to permit teleworking included "*client requirements, role in business continuity processes, project management roles*." Mgt_1 added that the teleworking was principally for employees in "*client-facing/project delivery roles*."

Mgt_2 added that the teleworking was permitted in their unit for "*employees who were eligible for laptops. Typically, team leads and above*." It appeared that Mgt_3's unit had stricter norms for allowing teleworking, due to their clients:

> "*Yes, teleworking was allowed before the pandemic based on approval. Since our unit is for financial clients, we did not generally encourage telework. However, when required for business continuity reasons we made sure that the concerned employees were using only company-provided laptops which were configured as per the client specifications.*"

Sub-theme 2: Roles/jobs better suited for teleworking

The narratives of the management team provided insights regarding the roles/jobs better suited for teleworking. Mgt_1, for instance, indicated that teleworking was most appropriate for roles which could be performed unsupervised or for work assignments where the scope and deliverables were clearly delineated:

> "*To be honest, I feel roles that don't need constant supervision are most suited for teleworking. Also, I feel employees with certain years of experience and proven track record at work. It helps if the work scope is clearly defined and there are specifications regarding deliverables and deadlines.*"

Mgt_3's opinion was also aligned with his colleague as he also believed that clearly defined tasks were essential for teleworking. Moreover, he added a further dimension when he highlighted that collaboration inserted complexity into a teleworking scenario:

> *"Roles with clearly defined tasks are best for teleworking. It is a stretch for a project team where everyone must collaborate and there are task dependencies."*

The narrative of Mgt_2 indicated that she supported this latter thought process as she specified that roles which could function autonomously were more suited for teleworking:

> *"I feel roles that don't have a lot of dependency on other roles are the best suited for teleworking. Also, I feel there has to be a certain amount of job-related maturity before a person can work independently from home."*

Sub-theme 3: Organisational Support for telework

The narratives of the interviewees provided details of the organizational support for telework. One aspect of the support involved the provision of facilities or infrastructure to support teleworking employees. For example, IT_1 highlighted that prior to the pandemic, employees were eligible for client devices and reimbursement of telephone/Wi Fi bills based on role/grade or project requirements. However, after the pandemic, due to the limited reach, employees were allowed to purchase client devices for use during telework. In IT_1's words:

> *"We were providing client devices to employees based on their role/grade and for specific project requirements. Also, we used to reimburse telephone/Wi Fi bills, again as per limits for different roles/grades. Since the pandemic took everyone by surprise, we were forced to allow employees to purchase and use their own client devices. Also, to support the employees we paid for Wi Fi connectivity for a period of six months."*

From IT_2's narrative, it appeared that employees were also permitted to take their workstations home. That is, it appeared that employees who were not eligible for laptops were permitted to take their desktops and associated accessories to their homes:

> *"We were providing client devices to employees based on their role/grade and for specific project requirements. During the pandemic we allowed employees to take their workstations to their homes."*

IT_3 added that "*Client devices were provided to employees based on their role/grade and for specific project requirements*."

As may be expected, the management team had their own insights to contribute in this regard. For example, as described by Mgt_1, the employees were permitted to use their own devices to telework during the pandemic which necessitated a change in the telework policy:

> *"Before the pandemic, employees in team leader (or equivalent) grade were eligible for company-provided laptop and mobile device. After the pandemic started, employees were allowed to use their own devices to connect to the corporate network. IT team provided some software and patches for connectivity to the network. Also, they were asked to invest in some good VPN software...I know of some companies who reimbursed expenses related to*

> *setting up the home office, but this was not very practical for us as the number of employees in India alone is more than 100,000."*

According to Mgt_2, the facilities provided to teleworking employees was limited to reimbursement of expenses related to setting up a home office:

> *"We were allowed to approve reimbursement of some purchases for employees who had to set up their home offices. For example, internet connection. We did not reimburse for purchases of laptops/mobiles."*

The narrative of Mgt_3 highlighted that the nature of the client had an impact on the support for teleworking. Nevertheless, the reimbursement of certain expenses seems to have been a standard matter in the organization. As he mentioned:

> "*Since we are working for a financial services client, we had to arrange for client devices to be sent to the employees in the account. Employees were asked to purchase their own internet connection. Expenses were reimbursed for a few months.*"

The IT team provided further detail about the facilities provided by them for teleworking employee. For instance, IT_1, IT_2, and IT_3 drew attention to the service desk provided to assist teleworking employees. IT_1 mentioned that employees could raise a ticket for assistance with installations, software bugs, troubleshooting for in-house applications. In addition, a helpline was also provided for emergency assistance.

IT_2 and IT_3 highlighted, additionally, that all teleworking employees have to install a client which could help the IT team monitor their connection to the organization network.

The management team correspondingly provided insights regarding the support they provided for the teleworking employees. For example, Mgt_1, speaking at the organisational level highlighted that:

> *"To keep the employees engaged, we organised monthly town halls with the leaders. Also, HR team hosted some weekly sessions related to productivity tips, health, ergonomics/posture. We even conducted some online quizzes on different topics and held some competitions. Just to keep the energy going and to make the employees feel more connected with each other even though they were physically distant.*"

On the other hand, Mgt_2 and Mgt_3 highlighted the support provided at a more granular unit/project level. As Mgt_2 said:

> "*Apart from the regular meetings set up by HR at the organisation level, at the unit level we had some town halls. Teams continued with team meetings. Project managers and team leaders held weekly interactions with individuals to ensure that they understood the work specifications and to help them if they were stuck anywhere. I conducted meetings with my managers to understand progress and discuss solutions for any challenges due to teleworking.*"

Mgt_3 said:

> "*There are some meetings at the organisation level set up by HR. In our unit, the unit head set up monthly town halls. In our account, the client also set up some town halls just to keep up the morale of the team. I set up some meetings with my immediate team (project managers and team leaders) to understand the challenges they were facing and what their teams were communicating. I also held interactions with groups of individuals to check their progress during teleworking. Whether they needed any kind of support from the organisation, not just work-related. In addition, I encouraged the team to have weekly project meetings to ensure that work specifications were clearly communicated and tracked.*"

Sub-theme 4: Tools used during teleworking

The management team narratives indicated the tools utilized during teleworking to communicate with the teams. For example, Mgt_1, speaking at the organizational level mentioned that "*We investigated use of many tools and finally decided on Microsoft Teams*." Mgt_2 and Mgt_3 corroborated that Microsoft Teams was utilised for all meetings as specified by the organisation. In addition, they also used direct phone calls for personal (one-on-one) discussions.

4.4.2 Theme 2: Impacts of telework

The second theme was related to the perceived impacts of telework. Six sub-themes could be identified in relationship with the second theme namely, Productivity in teleworking; Support for productivity; Changes to teleworking policy; Managing files and data; Cybersecurity risks and threats; and Security and teleworking.

Sub-theme 1: Productivity in teleworking

The management team had different perspectives of the term productivity. For example, while Mgt_1 believed that it meant "*that there is no delay to customer deliverables*," Mgt_2 believed that it signified "*employees meeting project deadlines*." In contrast, productivity was a combination of output and efficiency to Mgt_3:

> *"That is, the number of hours an employee takes to complete a task and how well they manage their time."*

Unsurprisingly, they had some definite opinions regarding the productivity of the employees when teleworking. Overall, it appeared that there were some fluctuations in the productivity. At the organization level, Mgt_1 mentioned that there had been no customer complaints. However, she was aware of some issues related to the productivity of team members, though some of the problems seemed to be related to infrastructure and could be sorted out easily. Other issues required more serious intervention:

> *"We had no customer complaints overall that I know of. But I know that some managers had to escalate that few of their team members were not completing their work on time. Some of this was sorted out by asking them to change their Internet provider. For some others we had to recommend more supervision and even disciplinary action was taken which reflected eventually at the time of the employees' performance appraisal and compensation reviews."*

Mgt_2's opinion indicated the initial impacts to productivity at the start of the pandemic. She believed that things had settled down subsequently. However, she seemed to believe that teleworking had a negative effect on employees' productivity:

> *"On the whole productivity was definitely impacted, negatively. At least in the early days of the pandemic when we were still trying to figure out who was able to telework immediately and we were working out the details of connecting to the organisation network. After that it has settled down, except for a few exceptions."*

This negative opinion was shared by Mgt_3 who said:

> *"There is a negative trend. Some employees are able to continue to deliver efficiently while others have lagged behind."*

Relatedly, the perspectives of the management team revealed factors that they believed could influence the productivity of employees. The factors included deliverable type, timelines, understanding of the work, dependence on other team members, infrastructure, lack of guidance, lack of communication, among others. For example, in Mgt_1's opinion:

> *"Employee productivity can be impacted by the kind of deliverable, the timelines to be followed, their understanding of the work, the level of*

> *dependence of their work completion on other team members. During the pandemic, one additional impact was due to network connectivity – both speed and stability."*

In addition, Mgt_1 highlighted that some of the impacts due to infrastructure were based on the location of the employees.

> *"Some of the employees had moved to smaller cities/towns and the network infrastructure there was not as good as in Bangalore and Chennai, for example."*

The opinion of Mgt_2 revealed that apart from technological issues, other people could impact the productivity of an employee. For example, dependencies on other team members or waiting for guidance from a leader could impact an employee's productivity:

> *"Some things that affect employee productivity include technological issues; lack of leadership from the project leaders; lack of interaction with the rest of the team as sometimes people don't know what is happening with the team members. Also, if there is some delay from one team member it can impact the rest of the team."*

Mgt_3 noted that the overall work environment had a significant impact on productivity. Other factors included personal characteristics of employees and the technology:

> *"Factors that affect productivity include the environment of work, opportunities for training and career development, the organisational and project process, pay. Some other factors are communication, how people manage their time, technology available for use."*

Sub-theme 2: Support for productivity

The management team's narratives also highlighted whether the use of VPN could support the productivity of the employees when they are teleworking. Mgt_1, for example, had some reservations about the contribution of VPN in this regard:

> *"I'm not so sure if VPN has some role to play in productivity. But surely it can help reassure the employees that their laptop/mobile device is safe when connecting to the company network and so they can work peacefully. The stability of the network connection may have more to do with productivity to be honest."*

Furthermore, Mgt_2 noted that VPN could help monitor login hours. However, in her opinion, the productivity itself was more dependent on the efficiency of employees:

> *"If employees connect through VPN to the corporate network, we can keep track of the amount of time they are logged on. So, this can help us check if an employee logs the required number of login hours per week/month. However, from a purely delivery perspective productivity is more related to how efficiently the employees work to complete their deliverables. It is related to how well the employees collaborate with their colleagues and managers."*

Mgt_3 also emphasized the contribution of VPN to track employees' login hours. It appeared that the management was interested in monitoring login time to measure productivity.

> *"VPN supports secure connections so employees don't have to worry about their data. In addition, the organisation can keep track of login hours."*

Sub-theme 3: Changes to teleworking policy

As could be expected, the case organization had to revise its policy for telework based to support employees during the pandemic. As mentioned by Mgt_1:

> "*After the pandemic lockdowns were announced, we had to make arrangements for all employees to be able to work from home regardless of their role. The policy was extended to include this*."

Moreover, she mentioned that the policy was extended to support the usage of personal devices:

> *"We revised the telework policy to include use of personal devices and also included reimbursement for Wi Fi bills for a few months."*

Mgt_1 and Mgt_3 added that this reimbursement was already in the existing policy for employees of management grade and higher. As mentioned by Mgt_3:

> *"There is a policy for reimbursement of Wi Fi and telephone bills, up to a specified limit based on job grade."*

However, Mgt_1 indicated that this was now extended to all employees. She also highlighted her awareness of some of the practices of other organisations, while noting that these were not implemented in the case organisation:

> "*…some companies reimbursed expenses related to setting up the home office, but this was not feasible for us due to the large number of employees.*"

Mgt_2 anticipated that the reimbursement policy would be revised soon as the pandemic was now over.

> *"Reimbursement of Wi Fi and telephone bills was already in the policy for all employees during the pandemic. I expect this will be changed soon."*

IT_1 also added that the policy was extended due to the pandemic to allow all employees to telework.

Sub-theme 4: Managing files and data

The management team narratives indicated their different levels of knowledge regarding the management of files and data utilised by teleworking employees. Mgt_1, who is in Human Resources, admitted that she was not very aware of the specific details of this. However, she was aware that the IT team has set up some tools and processes for this.

Mgt_2 and Mgt_3 demonstrated greater awareness, perhaps due to their involvement in actual client deliverables. Mgt_1, for instance, mentioned:

> *"We have dedicated servers and file storage for each client in the unit. The IT team created tools and utilities that could be used through a VPN connection to access the files. The employees had to log in using their company user name and password. A secure token was also generated for every session."*

Mgt_3's narrative was on similar lines. However, due to his engagement with a financial services client, it appeared that the management of files and data for his unit was more stringent:

> *"Our clients have very clear specifications about files and data related to their projects. So we directly use their servers and file storage. The employees have to log in using their client-provided user name and password. Internal files are stored on the cloud storage allocated for our unit."*

The IT team's perspective was more technical, as can be expected. For example, IT_1 mentioned that they:

> *"insist on encrypting the storage of devices, encrypting any sensitive data stored on client devices."*

This was confirmed by IT_2 who added some insights regarding the organisation's security measures:

> *"Security measures used in the organisation include secure configuration of workstations, client devices, prevention of malware, network security measures, user awareness and training."*

IT_3 also confirmed the encryption of device storage and data. In addition, he provided insights regarding other measures:

> *"Other measures include secure configuration of workstations, client devices, prevention of malware, network security measures, user awareness and training. We tried to educate all employees about the security policies especially as the switch to "work from home" was quite sudden. Specifically, we had to highlight and enforce use of authorised software and hardware."*

Sub-theme 5: Cybersecurity risks and threats

The narratives of the IT team revealed insights regarding the cybersecurity risks and threats faced by the organisation. These encompassed application, network, and cloud security. In addition, all of them revealed concerns regarding "*Phishing attacks, malware, ransomware*." IT_1 added the concern about hackers:

> *"Hackers gaining access to sensitive information such as, user account details, users' personal information, client data, company financial data."*

Relatedly, the main cybersecurity challenges encountered by the organisation's clients were revealed to be primarily related to their data (financial and application) as reported by IT_1 and IT_2. IT_2 additionally highlighted the threats to network security.

IT_3 provided more detail in his narrative:

> *"Basically, there are some common challenges encountered by all clients. For example, poor endpoint device security, lack of security awareness, etc. Some specific challenges include slammer worm attacks, malicious hacking,*

> *malware attacks, phishing attacks, Distributed Denial-of-Service (DDoS) attacks, data breaches, ransomware attacks, data break on mobile apps, cryptocurrency mining malware, and software errors. Another aspect of cybersecurity is human error."*

The narratives of the IT team also provided some insights regarding the security of the organisation's/clients' data when employees are teleworking. For example, IT_1 believed that the use of VPN products was beneficial for data security:

> *"I feel the data can be secure if the employees are using a VPN product to connect to the organisation/client network."*

This opinion was confirmed by IT_2, who also commented on the organisation's policy for connections from outside the organisation network:

> *"Data can be secure if the employees are using a VPN product to connect to the organisation/client network and the organisation has a clear policy for external connections."*

IT_3's narrative was more detailed as he highlighted the compliance of the organisation to Indian cyber law. He also shared the opinion of his colleagues regarding the usage of VPN products and highlighted the policy for external connections.

> *"Our organisation follows the parameters of due diligence is compliant with all applicable requirements, rules, and regulations under Indian cyber law. In addition, since we specify that the employees must use a VPN product to connect to the organisation/client network, the risk to client data is reduced. In addition, our organisation has a clear policy for external connections."*

Sub-theme 6: Security and teleworking

The management team indicated their different levels of knowledge regarding security measures utilised by the organisation to support teleworking. For instance, Mgt_1 felt that the IT team was better equipped to deal with the matter and also to provide information regarding this as she said: "*I think the IT team is better equipped to answer this question*." However, she was aware of the protocol to log in to the office network:

> *"I know they asked all of us to install VPN on our laptops and to use a portal to connect to the office network. We have to login using our login ID and password, together with a secure pin."*

Mgt_2 seemed to be more aware as she said:

> *"All employees have to have VPN on their laptops, this is particularly for employees who are using their own devices to log in to the company network. They have to use a portal to connect to the office network. Access to the company network and resources is obtained by using login ID and password, together with a secure token."*

Mgt_3 also seemed to have a greater awareness of the security measures. This could be because of the greater requirements from their client/line of business for security:

> *Access control through user ID and password to the organisation network and resources. All laptops used for company work have to have VPN installed. Organisation uses a cloud-based VPN to provide a secure connection. In addition, because we are working for a banking client we have client-provided user IDs and passwords to access client sites.*

The IT team added their perceptions regarding the security of data when employees are teleworking by highlighting the contribution of VPN. In IT_1's opinion, VPN helped by ensuring safe sharing of files and securing remote access to the network:

> *"VPN helps the organisation to support teleworking while ensuring that files are shared safely, remote access to the organisation network is secure"*

The narrative of IT_2 revealed his firm belief in the benefits of using VPN to safeguard data:

> *"By using VPN technology and VPN gateways with personal equipment, users can understand that their machines are connected to the firm's network, and as such are subject to the same rules and regulations that apply to firm-owned equipment, i.e., their machines must be configured to comply with the company's security policies."*

On the other hand, IT_3 revealed his awareness of the limitations of VPN

> *To be honest, in my opinion, the security offered by VPNs is limited. But this is the simplest way to avoid some of the technology-related risks associated with teleworking. For instance, it typically ensures the security of the employee's connection to the organisation network by encrypting the data.*

The narratives of the IT team provided insights regarding how the organisation dealt with the security requirements when employees used their own devices to connect to the organisation network. For example, IT_1 mentioned that the VPN usage policy covered this situation:

> *"We have a clear VPN usage policy which describe the policies for users who have to use their own devices."*

IT_2 added details about the aspects of the policy:

> *“Only approved VPN clients may be used. The VPN connection can last only up to 24 hours at a time. After 30 minutes of inactivity, VPN users will be automatically disconnected from the organisation network.”*

IT_3 acknowledged that security was a concern due to the inability to physically monitor the devices. However, he believed that they were able to achieve some measure of control through the policy specifications:

> *“It is certainly a difficult thing to achieve since physical security controls or file encryption may not be possible. Even ensuring regular backups is difficult. However, we try our best by insisting that only approved VPN clients may be used. The VPN connection can last only up to 24 hours at a time. After 30 minutes of inactivity, VPN users will be automatically disconnected from the organisation network. We also have setup a reminder for employees to backup their local files to a centralised storage system.”*

It could be seen that the VPN usage policy of the case organisation included provision to regulate the duration of the VPN connection and also, to monitor inactivity. However, employee compliance to the policy would be required.

4.4.3 Theme 3: Facets of VPN usage

The third team was related to VPN usage. Four sub-themes could be identified in relationship with this theme namely, VPN features; VPN and teleworking; Benefits and risks of VPN usage; and Factors to be considered prior to continued VPN use.

Sub-theme 1: VPN features

The IT team provided some insights regarding the VPN provider used by the organization. Overall, it appeared that the organization used a custom secure remote access VPN solution. Employees were permitted to use any VPN client software to connect.

The criteria to choose this VPN solution included speed (quality of service), the price of the service, its ease of understanding/usage, its features, the ability to change location to access media on websites; number of servers located around the world; and clear explanation of logging and data practices. Overall, the IT team highlighted that most of these aspects were "*Required*" except for "Speed (Quality of service)" and "Easy to understand/use app (GUI)" which were tagged as "*Preferred*" by IT_1. "Price of the service" was tagged as "Preferred" by both IT_1 and IT_3.

The security features of the VPN solution utilised by the case organisation included robust security features. Also, it had a large and distributed network of servers. IT_3 summed it up when he said that their VPN solution had a:

> *"large and distributed network of servers, robust security features such as, threat protection, dark web monitor, split tunnelling. We ensured that an auto-connect feature was included"*

Sub-theme 2: VPN and teleworking

The narratives of the IT team revealed insights regarding how VPN supports teleworking employees. Overall, VPN was used to provide secure access to the internal network and data as reported by IT_1 and IT_2. IT_3 added,

> *"By insisting on VPN use, we can ensure that employees have online privacy and digital security not only when they are connected to the organisation network but also when they are using the same client device for personal matters."*

The IT team confirmed also that VPN use was mandatory for teleworking employees. According to IT_1 this was because "*we can't risk external attacks*." IT_2 and IT3 confirmed that this specification was "*part of the guidelines for telework*."

It appeared that teleworking employees could use any VPN provider from a list of recommended providers as mentioned by IT_3. The others merely stated that the employees could use any provider they wanted. In addition, it appeared that the organisation had sufficient gateways for remote access. As summed up by IT_3:

> *"They can use any provider they want from a list of recommended providers. We have provision for adequate VPN gateways for remote access."*

The management team also had some insights regarding how VPN was used to support teleworking employees. For example, it could be seen that Mgt_1 had a high-level understanding about VPN's features but she knew that it could help secure connections and data:

> *"Hmmm, I don't know the exact technical details. In my understanding, we are using VPN to protect the connection from an external network to the company network. I guess it has some features to protect the data as well."*

On the other hand, Mgt_2 was a little clearer about VPN and how it supported teleworking:

> *"Using VPN means that the employees can log on to the company network from anywhere in the world as long as they have Internet access. VPN also supports access control, so users can be granted access only to what they absolutely need to access. In addition, it is a means to ensure a secure private communication through public networks."*

A similar opinion could be seen in Mgt_3's narrative:

> *"VPN helps employees log on securely to the company network from anywhere in the world. VPN supports access control, so the organisation can ensure that users are granted access only to what they need to access."*

The IT team also provided some insights regarding the precautions to be taken at the organisation side as employees could choose their own VPN provider. One precaution was through a specific policy for VPN usage as described by IT_1:

> *"We have a clear VPN usage policy which describe the policies for users who choose their own VPN options."*

IT_2, on the other hand, drew attention to the authentication protocol and need for anti-virus software:

> *"Connectivity to the organisation network must be controlled by using a one-time authentication such as, a token or key. VPN gateways must be set up by the IT team. All client devices connected using VPN must have the most up-to-date anti-virus software as specified by the organisation."*

A very detailed narrative was provided by IT_3, who confirmed what his colleagues had mentioned about the precautions to be taken for VPN use:

> *"Some of the precautions we have implemented are the use of one-time authentication such as, a token or key, to control connectivity to the organisation network. We have used multi-factor authentication combining user ID/pin and secure token. For employees working with high-security clients, we have also ensured biometric identification as these employees are typically using client devices provided by the organisation. In addition, the IT team has set up VPN gateways. Also, all client devices connected using VPN must have the most up-to-date anti-virus software as per the organisation's specifications."*

Sub-theme 3: Benefits and Risks of VPN usage

The narratives of the IT team revealed also their perspectives regarding the benefits and risks of using VPN in the organisation. In IT_1's perspective, the benefits were that:

> *"Employees can telework from any part of the globe as long as they have VPN. Online privacy is protected; data is encrypted."*

On the other hand, he highlighted that VPN was not very safe as it "*can still be hacked*." Also, they had to grant permissions for sensitive resources to be accessed through VPN which increased the risk.

IT_2 felt that the use of VPN could ensure security of data and privacy of the employees' connection to the office network:

> *"We can ensure that only traffic intended for the organization travels across the VPN gateway. All other traffic is directed through the user's internet service provider (ISP). By insisting on VPN we can ensure that data is secure when teleworking employees access them."*

Nevertheless, he believed that VPN use could slow down the connection which it may be inferred adversely impacted productivity. Furthermore, an unreliable connection could increase the threat to the company network. An additional aspect highlighted by IT_2 was that VPN can be difficult to configure:

> *"VPN can slow down the network connection. Sometimes they can even result in the connection being dropped which exposes the network to threat. Also, some options are difficult to set-up."*

Finally, IT_3 also drew attention to the security aspects of VPN when he mentioned that by insisting on VPN, the security of data could be ensured "*when* *teleworking employees access them due to the encryption feature of VPN*.” However, he also highlighted the possibility of slow connections due to VPN use:

> *“VPN can slow down the organisation network. The bandwidth of the network can be reduced due to the high number of VPN connections.”*

He also added that an interrupted VPN session or the failure to use VPN even for a short period could mean that a client device was unsecured and could prospectively impact the organisation network:

> *“…VPN is not always fool proof. If an employee fails to use VPN to connect, this may mean that some of the patches we specified are not installed in time and the device becomes unsecured.”*

The opinions of the management team also revealed what they thought about the pros of using VPN. Mgt_1’s opinion revealed that she believed that VPN helped keep data safe. On the other hand, she mentioned that it could be unreliable:

> *“Can be unreliable. I myself encountered several instances of where the VPN connection would time out and then I would have to log in again into the corporate network.”*

Mgt_2, on the other hand, commented favourably about the privacy aspect of VPN:

> *“The privacy of the connection makes it possible for employees to continue with client projects. Some of our clients own the intellectual property on their manufacturing processes and products, so it is essential that these remain confidential.”*

However, she also highlighted that VPN was not completely safe as it could be hacked. Moreover, they were depended on Internet connectivity:

> *“Can be hacked. So that prospective danger is also there. Also, because they are dependent on an Internet connection, the stability of the connection can*

> *fluctuate if there are problems with the network. During these downtimes, the risk to the data is so much higher."*

Mgt_3, again, highlighted the security aspect. Additionally, he highlighted that VPN use could help track productivity of employees since the connection start and end times could be monitored:

> *"We are able to support banking clients who need a very high level of security. In addition, we can keep track of login hours."*

However, he highlighted that it was not completely secure. Furthermore, he introduced a new concern regarding VPN usage in different countries:

> *"VPN is not 100% secure. Not all VPN clients can create policies to safeguard user credentials. Also, some countries don't allow VPN, so that also has to be considered."*

Sub-theme 4: Factors to be considered prior to continued VPN use

The IT team indicated that in the continuing context of telework, certain factors needed to be considered. For example, IT_1 mentioned the need to continuously monitor guidelines and update policies related to VPN:

> *"Clearly, we have to keep track of international and national guidelines for network and data security and continuously update our policies."*

IT_2 highlighted the need to consider synchronisation of devices along with other factors in the context of partial telework:

> *"We will have to see how to manage a partial telework model and how to ensure synchronisation between client devices as employees may use different devices in the office and at home. The other thing is that we will have to keep*

exploring options to ensure security of data during remote access. We may look at enforcing certain VPN products as well."

The additional considerations due to partial telework was also highlighted by IT_3:

Currently, we are asking employees to come to office a few days a week at least so we are working on a partial telework model. Now the challenge is to manage the use of different client devices at home and at the office. We will continue to require employees to use VPN to connect client devices from their home networks. VPN products have continued to evolve, so we will probably be looking at standardising usage of certain products.

The management team also highlighted the need for clearer VPN options and the need to support personal client devices. As Mgt_1 said:

"Well, we will have to be very clear about the VPN options that employees can use as some are more reliable than the others. Also, the IT team may have to come up with some tools to support personal client devices. The pandemic has taken BYOD to another level, seriously. And I feel there is no looking back as we have not been very successful in enforcing full-time return to the office so far."

Mgt_2 suggested the need to explore different configurations of VPN to support different frequencies of teleworking:

"The organisation will certainly have to explore different VPN configurations to support full-time and part-time teleworkers. Cloud-based VPN infrastructure is already being used, but we don't have much control on the client side as some employees are still using their own devices. This has to be evaluated."

Security was Mgt_3's principal concern. He also suggested the check of other options for VPN and establishing a team for teleworking-related VPN:

> *"Ensuring optimal security. Checking cloud and hybrid cloud options. A separate team may be needed only for VPN related to teleworking."*

4.5 Summary of Findings

Quantitative Findings

Participant demographics

- The majority (54.5%) of the participants were in the age group of 31 to 40 years.
- The majority (58.0%) were male
- The majority of the participants were Graduates (83.5%)
- The majority of the participants had worked for <5 years (34.5%) in the organisation
- The majority of the participants were full time employees of the case organisation (85.0%).

Teleworking experience

- The majority of the participants had commenced teleworking only during COVID
- After the pandemic, the majority of the participants were continuing to telework.
- After the pandemic, the majority of the participants were teleworking 3 days a week or less

- The majority of the participants were using facilities provided by the case organisation for teleworking
- The facilities provided by the firm included personal computers and secure connectivity
- The majority of the employees believed that their data were very secure when teleworking
- The majority believed that the firm was responsible for the security of their client devices
- The most popular security measures used were "Requires a password/passcode and/or other authentication before accessing the organization's resources" and "Regular application of device manufacturer updates and patches to protect devices from known vulnerabilities"
- The employees believed they were more productive at home
- The majority indicated that they would like to continue teleworking and supported more telework.
- The most common channels of communication utilised during teleworking were email, chat/instant messaging (e.g., Skype, Microsoft Teams, etc.), and video (e.g., Zoom, Microsoft Teams, etc.)

Productivity while teleworking

- Job Role: The employees were clear about their job role as the data indicated that they agreed that they were clear about what is expected of them at work; they were clear what their duties and responsibilities were; and they understood how their work fits into the overall aims of the organization

- Job performance: The employees agreed that they felt that they have been effectively fulfilling their roles and responsibilities when teleworking and their overall performance is very good/outstanding when teleworking
- Work autonomy: The employees agreed that they were allowed to plan how to do their work; they were allowed to use their personal initiative or judgment in carrying out the work; they were allowed to make decisions about what methods they use to complete their work; they have considerable opportunity for independence and freedom in how they do the work; and they were allowed to decide on their own how to go about doing their work.
- Work complexity: The employees agreed that their job tasks were intricate and complex; required that they engage in a large amount of thinking; required them to keep track of more than one thing at a time; required the use of a number of skills; were highly specialized in terms of purpose, tasks, or activities; required very specialized knowledge and skills; and required a depth of knowledge and expertise.
- Perceived productivity: The employees indicated that their productivity at work has improved while teleworking despite greater number of meetings and other communication; that they were more efficient in their work when teleworking; they were able to collaborate well with peers while teleworking; and were able to obtain guidance and feedback from their manager while teleworking.
- Productivity level: The majority of the employees agreed that their productivity during teleworking was Hugely better or Substantially better

- Organisation measure of productivity: The majority of the employees agreed that their organisation sets and communicates clear goals and deadlines in the same way as they do with workers in a physical workspace; has formed plans to increase their accountability; analyses important tasks and track progress on a time bound basis; evaluates quality and quantity instead of time worked; has shifted metrics from "hours spent" to "tasks accomplished and their quality"; and tracks their achievements

VPN and teleworking

- The most popular VPN options used by the employees were ExpressVPN (used by 16.0%), NordVPN (used by 11.0%), and Hotspot (used by 10.5%).
- The employees' most popular reason for choosing a VPN solution was that it was provided to them by the organisation.
- The majority of the employees were not concerned about the type of VPN subscription as it was provided by the firm
- The employees' purpose of using a VPN product was mainly for file sharing, to access their work network, and to access region-specific content
- Most of the employees used VPN all the time
- VPN and productivity: The employees agreed that VPN helps secure their connection to the organisation network; VPN helps with productivity in teleworking; and they do not have to worry about the security of their data.

- Awareness of VPN concept: The majority seemed to be aware that it is a network that can be connected remotely and it is an application for information privacy and security.
- VPN functioning: The employees were aware that it is a subscription-based model; uses a high-speed leased line; and with VPN, dial-up modems can be used to connect remote locations to the Internet.
- VPN risks: The employees were aware that Hackers and computer thieves can decrypt VPN connection; VPN applications require access rights to sensitive resources such as user accounts; VPN applications contain malware that affects the security of the operating system; VPN applications collect users' personal information and sell them to external partners; VPN applications allow sharing the IP address given by the application with other users; VPN applications direct the browser to websites without your permission; and VPN applications steal network bandwidth and resell it.
- VPN advantages: The employees were aware that VPNs eliminate geographical restrictions; Online privacy is safeguarded; My connection is protected from cyber criminals; Regional leased lines or even cable networks can be used to connect to the internet; Cost saving; and Uses public networks to tunnel a private connection.

Influence of participant demographics on work features, productivity, facets of VPN usage

- Employee perceptions regarding Job Role were found to be influenced by their Gender

- Perceptions regarding Job Performance were found to be influenced by Nature of employment
- Perceptions regarding Work autonomy were found to be influenced by Age, Educational qualification, and Work experience
- Perceptions regarding Job complexity were found to be significantly influenced by Gender and Work experience
- Employees' perceptions regarding Perceived productivity were influenced by Nature of employment and Work experience
- Employees' perceptions regarding VPN and productivity were influenced by Gender, Educational qualification, Nature of employment and Work experience.
- Employees' perceptions regarding their Awareness of VPN concept were influenced by Age, Educational qualification, Nature of employment and Work experience
- Employees' perceptions regarding VPN Functioning were influenced by Age
- Employees' perceptions regarding VPN Risks were influenced by Gender
- Employees' perceptions regarding VPN Advantages were influenced by Educational qualification and Work experience.

Impact of work features and facets of VPN usage on productivity of teleworking employees

- Some aspects of work features (i.e., job role, work autonomy, and job complexity) have a positive impact on productivity of teleworking employees

- Certain facets of VPN usage (i.e., VPN and productivity, VPN risks, VPN advantages) have a positive impact on productivity of teleworking employees

Impact of work features on facets of VPN usage

- Some aspects of Work features (i.e., job role, work autonomy, and job complexity) have a positive impact on facets of VPN usage

Qualitative Findings

Facets of Telework in the case organisation

- Teleworking had been permitted in the the case organisation prior to the pandemic and there was an associated teleworking policy in existence. The eligibility for teleworking was by job grade/role. Moreover, there were some stipulations as regards number of hours of telework allowed per month, approvals, usage of devices, exception cases, etc.
- The management team indicated that some roles/jobs are better suited for teleworking. For example, roles not requiring constant supervision, work assignments with clearly defined scope and deliverables.
- The case organisation supported telework prior to the pandemic by providing facilities/infrastructure such as laptops, mobile devices, and reimbursing some expenses for eligible employees. After the pandemic, employees could use their own devices and receive reimbursement for some expenses. In special cases, such as financial services clients, client devices were sent from the organisation to the employees.

- The IT team had set up a service desk and helpline to aid teleworking employees.
- From a management perspective, teleworking employees were supported through regular town halls and activities. Weekly interactions were held at the unit/account/project level.
- Microsoft Teams was used at the organisational level for communication.

Impacts of Telework

- Different managers had different perspectives of the meaning of productivity
- Teleworking seemed to have caused fluctuations, mostly negative, in employee productivity
- Factors impacting productivity include deliverable type, timelines, understanding of the work, dependence on other team members, infrastructure, lack of guidance, lack of communication, etc.
- VPN helped managers track productivity with regard to login hours.
- The policy for telework was revised due to the pandemic.
- Access to files and data were managed through the use of dedicated servers and file storage. In addition, the IT team created tools and utilities for employees to gain access to the data and files they required for their work.
- Security measures implemented by the organisation included encryption of data, and use of authorised software and hardware.
- Cybersecurity risks and threats concerning the organisation were phishing attacks, malware, ransomware, hacking.

- The IT team acknowledged the positive impact of VPN products on data security.

Facets of VPN usage

- VPN features that influenced choice of a VPN solution included speed (quality of service), the price of the service, its ease of understanding/usage, its features, the ability to change location to access media on websites; number of servers located around the world; and clear explanation of logging and data practices
- VPN supports teleworking by providing secure access to the organisation network and data even with employee-owned devices.
- Factors to be considered prior to continued use of VPN included the need to continuously monitor guidelines and update policies related to VPN; and the need to consider synchronisation of devices along with other factors in the context of partial telework

4.6 Conclusion

This chapter provided the outcomes of the analysis of the data collected for the study. The description of the case organisation was first provided. The outcomes of the statistical analysis were then presented followed by the findings from the interviews. The chapter concluded with a summary of the results.

CHAPTER V:

DISCUSSION

5.1 Chapter Introduction

This chapter presents the discussion of the key findings from the study in the light of existing literature. Subsequently, the findings are organised around the study's research questions. The outcomes of both the quantitative and qualitative data analyses are integrated to appropriately answer each question.

5.2 Discussion of Results

Teleworking has been practiced across different domains for many decades. However, it was not universally adopted due to its perceived lack of applicability across domains and jobs. The COVID-19 pandemic disrupted this status quo and resulted in it being comprehensively and nearly instantaneously adopted in businesses across the globe especially in knowledge-intensive business services and information and communication services, public and private organisations implementing it in the fields of education, public administration, and financial services (Mılası, González-Vázquez and Fernández-Macías, 2021; Nemteanu, Dabija and Stanca, 2021). While teleworking helped with business continuity, it also helped improve employee satisfaction and performance through reduced traveling, work flexibility, and increased work autonomy. Moreover, it helped improve work-life balance, reduce absenteeism and turnover intention, increase organisational commitment and various other benefits (Shardeshmukh, Sharma and Golden, 2012; Greer and Payne, 2014; de Vries, Tummers and Bekkers, 2019; Delanoeije and Verbruggen, 2019, 2020; Dima *et al.*, 2019; Golden and Gajendran, 2019). However, teleworking also could result in lowered interaction among teams, professional isolation, increased work pressure, relational conflicts, and enhanced stress leading to adverse work and performance outcomes (Shardeshmukh, Sharma and Golden, 2012; Song and Gao, 2018; Golden and Gajendran, 2019; Delanoeije and Verbruggen, 2020).

Teleworking is inherently dependent on technology to perform work activities. While the technology is context-specific, computers with software specific to the job, phones, other electronic devices, and remote access at high-speed to corporate databases, are essential for teleworking (Golden, 2009). Adding the need for security to the mix, VPN has become a vital component of the daily process of teleworking (Binkhorst *et al.*, 2022). Bucșă, (2020), for instance, drew attention three teleworking situations where VPN can be of use: usage of employer-provided equipment for data processing, usage of an employee's own system, and the usage of cloud technology.

In this context, the present study focused on the impact of VPN on productivity and security in teleworking. Using a mixed-methods, single case, case study research design, the study investigated the experiences of a case organisation which uses VPN to support their teleworking employees. Overall, the outcomes of the study were consistent with previous studies which have scrutinised teleworking in various contexts.

The case organisation was a large IT organisation in India with global operations and more than 100,000 employees. From the participants in the quantitative study, it was found that the majority of the participants had commenced teleworking only during the pandemic. This was confirmed by the findings of the qualitative study where participants the management and IT teams confirmed that teleworking had been an option before the pandemic only for certain job grades or roles, with exceptions requiring approvals. Moreover, there was an existing teleworking policy which had to be modified during the pandemic. Also, it seemed that the teleworking was voluntary in nature and based on individual agreement prior to the pandemic and this had changed during the pandemic (Belzunegui-Eraso and Erro-Garcés, 2020). After the pandemic, it could be seen that the majority of the participants were continuing to telework for 3 days a week or less. This indicated a change to a partial telework or hybrid model of functioning in the organisation which was in line with the findings of the OECD report on productivity (Criscuolo *et al.*, 2022).

The study found that employees utilised facilities provided by the case organisation for teleworking. The facilities provided by the firm included personal computers and secure connectivity. The management team indicated that the provision of client devices was typically when it was required for highly secure clients such as, banking clients. This differed from the typical setup during COVID-19 where only software was provided to teleworking employees (Belzunegui-Eraso and Erro-Garcés, 2020). Other facilities provided to the teleworking employees were a service desk and helpline established by the IT team.

In addition, the study found that the employees believed that their data were very secure when teleworking and that the firm was responsible for the security of their client devices. Security measures used by the firm included the requirement for a password/passcode and/or other authentication before accessing the organization's resources and regular application of device manufacturer updates and patches to protect devices from known vulnerabilities. The qualitative findings also confirmed that security measures were implemented by the organisation such as, encryption of data, and use of authorised software and hardware. The principal cybersecurity risks and threats concerning the organisation were phishing attacks, malware, ransomware, hacking. This indicated that the organisation was aware of the IT and information security challenges encountered with teleworking employees (Mannebäck and Padyab, 2021).

Regarding productivity, the employees believed they were more productive at home. Unsurprisingly, the majority indicated that they would like to continue teleworking and supported more telework. The employees also indicated that their productivity at work has improved while teleworking despite greater number of meetings and other communication; that they were more efficient in their work when teleworking; they were able to collaborate well with peers while teleworking; and were able to obtain guidance and feedback from their manager while teleworking. The majority of the employees indicated that their productivity during teleworking was Hugely better or Substantially better. Also, the employees indicated that the organisation sets and communicates clear goals and deadlines in the same way as they do with workers in a physical workspace; has formed plans to increase their accountability; analyses important tasks and track progress on a time bound basis; and evaluates quality and quantity instead of time worked. Moreover, the organisation has shifted metrics from “hours spent” to “tasks accomplished and their quality”; and tracks their achievements. These aspects indicated that the case organisation was adapting policies to track employee performance during teleworking. The management team, on the other hand, were of the opinion that employee productivity was adversely affected by teleworking due to various reasons such as, infrastructure, network connectivity, and the employees themselves. This conflicting perception regarding productivity was in line with findings of prior studies such as, Drumea (2020) who found that productivity during teleworking was lower than “in-office” efficiency in the context of public organisations, and Bhattacharya and Mittal (2020) who submitted that productivity could be impacted by the individual needs of teleworking employees.

Additionally, the study found that the employees were clear about their job role; and they felt that they have been effectively fulfilling their roles and responsibilities when teleworking and their overall performance is very good/outstanding when teleworking. Moreover, the employees appeared to have considerable work autonomy as they were allowed to plan the performance of their work. In addition, the nature of their work was typically complex, requiring significant thought and skill, etc. This finding was consistent with the findings of Golden and Rajendran (2019) who found that teleworking was favourable for employees with complex jobs or jobs involving limited degrees of interdependence. The perspectives of the management team seemed to be aligned with this as they did indicate that teleworking was more appropriate for tasks that were clearly defined or for persons who could work unsupervised.

Drumea (2020) also found that online communication (associated with IT, network connectivity, lower interactions with colleagues) could be a significant challenge during teleworking. The case organisation seemed to have overcome this to a certain extent by using different tools for communication such as, email, chat/instant messaging (e.g., Skype, Microsoft Teams, etc.), and video (e.g., Zoom, Microsoft Teams, etc.). In addition, the management appeared to be diligently pursuing communication through townhalls, meetings, etc., as a means to engage with the teleworking employees.

The case organization used a custom secure remote access VPN solution. The criteria to choose this VPN solution included speed (quality of service), the price of the service, its ease of understanding/usage, its features, the ability to change location to access media on websites; number of servers located around the world; and clear explanation of logging and data practices (Barker *et al.*, 2020). On the other hand, employees were permitted to use any VPN client software to connect. The employees' most popular reason for choosing a VPN solution was that it was provided to them by the organisation. Relatedly, the majority of the employees were not concerned about the type of VPN subscription as it was provided by the firm. However, this seems to be a misinterpretation of the organisation's guideline to use only approved VPN clients and the reimbursement of some of the teleworking expenses. Nevertheless, the employees' used a VPN product mainly for file sharing and to access region-specific content. Also, they used the product all the time. The study found that access to files and data were managed through the use of dedicated servers and file storage. In addition, the IT team created tools and utilities for employees to gain access to the data and files they required for their work.

In the opinion of the employees, VPN helped secure their connection to the organisation network (Barker *et al.*, 2020) and with productivity in teleworking. Also, they indicated that they do not have to worry about the security of their data. The majority seemed to be aware that it is a network that can be connected remotely and it is an application for information privacy and security. Moreover, the employees seemed to have sufficient awareness of features, risks, and benefits. The IT team also acknowledged the positive impact of VPN products on data security. The management team believed that VPN helped managers track productivity with regard to login hours.

Additionally, in line with many studies (Shardeshmukh, Sharma and Golden, 2012; de Vries, Tummers and Bekkers, 2019; Delanoeije and Verbruggen, 2019, 2020; Dima *et al.*, 2019; Golden and Gajendran, 2019; Fana *et al.*, 2020), the study found that some aspects of work features (i.e., job role, work autonomy, and job complexity) have a positive impact on productivity of teleworking employees. Moreover, certain facets of VPN usage (i.e., VPN and productivity, VPN risks, VPN advantages) have a positive impact on productivity of teleworking employees. Also, some aspects of Work features (i.e., job role, work autonomy, and job complexity) have a positive impact on facets of VPN usage. It is believed that the current study is possibly the first to investigate the impact of facets of VPN usage on productivity as well as the impact of work features on facets of VPN usage.

Overall, the study found that VPN supports teleworking by providing secure access to the organisation network and data even with employee-owned devices which was in line with the security goals for telework (NIST, 2016). Moreover, various factors needed to be considered prior to continued use of VPN included the need to continuously monitor guidelines and update policies related to VPN; and the need to consider synchronisation of devices along with other factors in the context of partial telework.

5.3 Discussion of Research Question One

The first research question of the study was: "What are the features of the usage of VPN by organisations to support teleworking employees? That is, how is VPN used by organisations to support teleworking employees?" It could be seen from the study's findings that the case organisation used a server-client form of VPN usage. At the organisation side, a custom secure remote access VPN solution was used as the VPN gateway. At the employee side, different VPN solutions were utilised such as, ExpressVPN, NordVPN, and Hotspot. The qualitative findings indicated that the IT team provided a list of approved VPN solutions for the employees to choose from. The principal reason for employees to use a VPN product was for file sharing, to access region-specific content and to access their work networks remotely. The VPN client also was continuously in use.

VPN features which greatly supported teleworking included:

- ability to connect to a remote network;
- information privacy and security;
- secure internet connection;
- digital anonymity; and
- encrypt internet connection

5.4 Discussion of Research Question Two

The second research question of the study was: “What are the risks and benefits of VPN usage in this context? That is, is the usage of VPN to support teleworking beneficial or risky for organisations?”

The principal risks of using VPN in a teleworking context included:

- VPN applications allow sharing the IP address given by the application with other users;
- VPN applications contain malware that affects the security of the operating system;
- VPN applications direct the browser to websites without permission;
- Hackers and computer thieves can decrypt VPN connection;
- VPN applications steal network bandwidth and resell it
- VPN applications require access rights to sensitive resources such as user accounts; and
- VPN applications collect users’ personal information and sell them to external partners.

However, the most critical risks seemed to be the possibility of hacking and the exposure of the organisation network to external risks in case of unstable connections.

On the other hand, benefits of VPN use were:

- Connection is protected from cyber criminals;
- VPNs eliminate geographical restrictions;
- Online privacy is safeguarded;
- Regional leased lines or even cable networks can be used to connect to the internet;

- Uses public networks to tunnel a private connection;
- Cost saving; and
- Data transfer is encrypted.

The chief benefit for the organisation seemed to be related to the safe sharing of files and data through encryption.

5.5 Discussion of Research Question Three

The third research question of the study was: “What are the facets of a conceptual framework to promote productivity and cybersecurity through VPN usage in organisations which support teleworking?”

As could be seen in Section 2.8, a preliminary conceptual framework was derived based on the review of literature and the telework/telecommuting success model (Siha and Monroe, 2006, p. 472). Based on the study’s findings, it can be assumed that VPN contributes to cybersecurity and productivity in a teleworking context. Figure 5.1 depicts the final visualization of the conceptual model to promote productivity and cybersecurity through VPN usage in organisations which support teleworking. The use of VPN has to be supported through an extended and robust policy for teleworking.

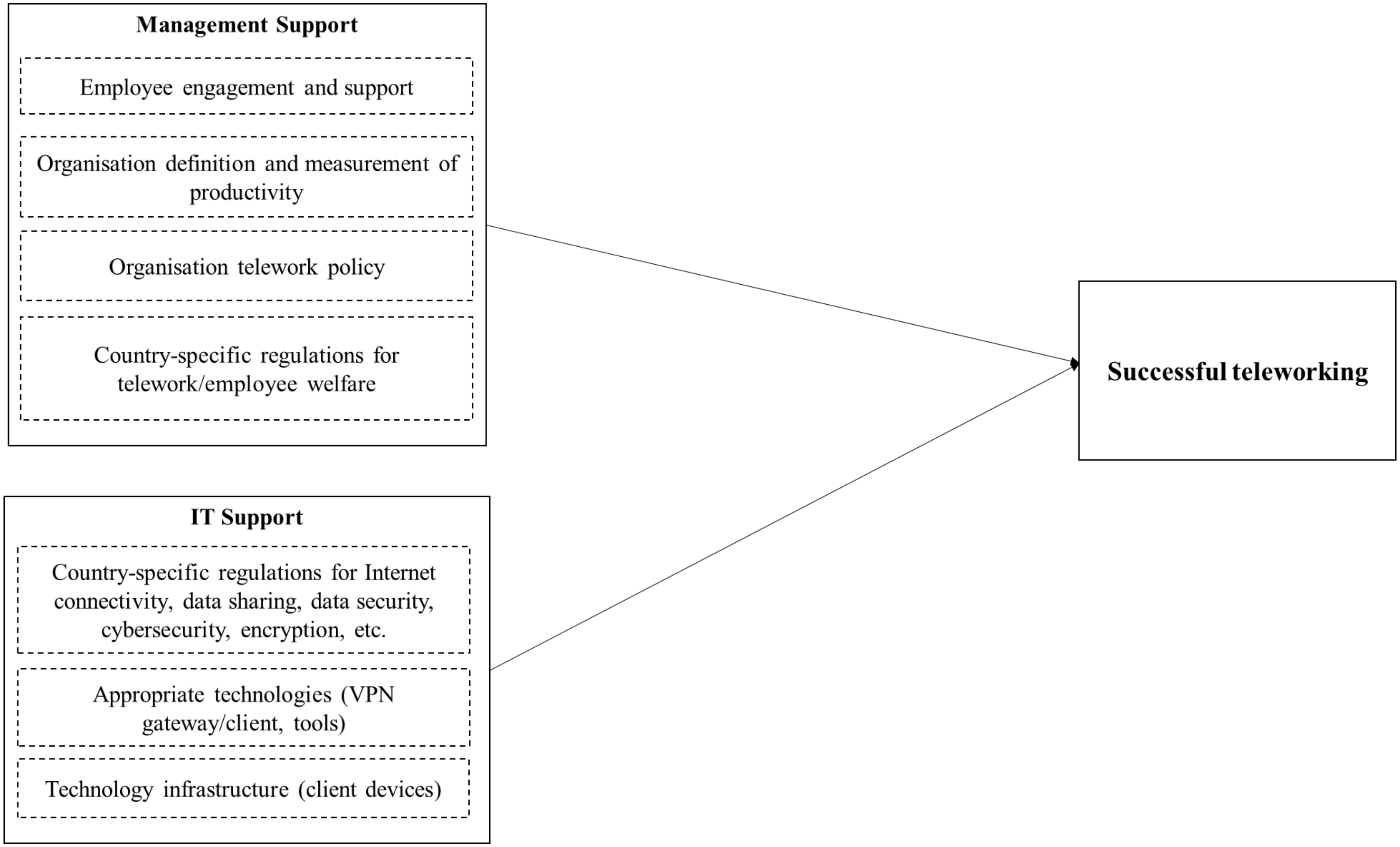
Management Support
Employee engagement and support
Organisation definition and measurement of productivity
Organisation telework policy
Country-specific regulations for telework/employee welfare
IT Support
Country-specific regulations for Internet connectivity, data sharing, data security, cybersecurity, encryption, etc.
Appropriate technologies (VPN gateway/client, tools)
Technology infrastructure (client devices)
Successful teleworking

Figure 5.1
Final visualisation of conceptual framework for productivity and cybersecurity during teleworking through VPN usage

5.6 Chapter Conclusion

This chapter presented the discussion of the key findings from the study in the light of existing literature. Subsequently, the findings were organised around the study's research questions. The outcomes of both the quantitative and qualitative data analyses were integrated to appropriately answer each question.

CHAPTER VI:

SUMMARY, IMPLICATIONS, AND RECOMMENDATIONS

6.1 Summary

Teleworking enabled businesses across the globe to survive the COVID-19 pandemic. In the present scenario, businesses are continuing to explore optimal combinations of telework and work-from-office to ensure productivity while ensuring that their data and resources are secure. Acknowledging the need for organisations to revisit and re-examine their experience with VPN usage to support extensive teleworking, this study focused both on the impact of VPN on productivity and security in teleworking, and also the learnings from the experiences of organisations who use VPN to support their teleworking employees.

The progress of this research to achieve the objectives of the study and answer the research questions was organised into six chapters. The first chapter, **Chapter 1 (Introduction),** provided the background for the study and introduced the perspectives of teleworking, teleworking standards, efficiency and productivity in teleworking, and technological support for teleworking. Moreover, it described the problem statement, identified the research question and objectives of the study, and highlighted the significance of the study. In addition, the key terms utilised in the study were introduced.

The second chapter, **Chapter 2 (Review of Literature)** offered a review of past literature associated with the theme of the current study such as, teleworking, productivity in teleworking, security and teleworking, VPN, and technology support for teleworking. The preliminary visualisation of the proposed conceptual framework was also provided in this chapter.

In the third chapter, **Chapter 3 (Methodology)**, the methodology adopted to achieve the objectives of the study was described. Since the researcher believed that the case study approach would be most appropriate in investigating productivity and security in the current post-COVID work context, the chapter described the case study approach along with the research design, instruments and processes adopted for this study. This included methods for collection and analysis of data, and techniques for sampling.

The fourth chapter, **Chapter 4 (Results)**, presented the findings of the study from the quantitative and qualitative elements of the case study. **Chapter 5 (Discussion)** discussed the findings of the study in the light of existing literature and answered the research sub-questions. In addition, the final visualisation of the proposed conceptual framework was provided. This final chapter, **Chapter 6 (Conclusion)**, will provide a summary of the study and its findings. In addition, the conclusions and implications derived from the findings will be highlighted. Recommendations will also be made based on the findings. Suggestions will also be provided for future researchers.

6.2 Implications

The following overarching research question was used to inform the study:

- Can productivity and security be achieved in the teleworking scenario in the post-COVID context through the usage of VPN?

Based on the findings from the case study, it is evident that VPN usage can facilitate productivity and security in the teleworking scenario. Productivity can be facilitated through the tracking of login hours. However, it must be noted that the organisational policy for teleworking must be correspondingly revised and extended to incorporate hybrid work arrangements, pure telework, and pure work-from-office.

Based on the proposed conceptual framework (Figure 5.1), a successful teleworking scenario in the post-COVID context can be stated to comprise two broad elements: Management Support and IT support. The management support comprises employee engagement and support; clearly defined facets and measurement of productivity; telework policy; and country-specific regulations for telework and employee welfare. Correspondingly, the IT support element includes consideration of country-specific regulations, appropriate technologies, and technology infrastructure.

Overall, teleworking helped with business continuity and improved employee satisfaction and performance due to the lowered traveling, flexibility of work, and enhanced work autonomy. The findings of the study have some implications that may be beneficial for companies.

6.2.1 General implications

- *Development of hybrid work models*: Companies can consider implementing a hybrid work model that integrates in-office and remote work, allowing employees to experience the advantages of teleworking while maintaining a sense of connection and collaboration with their colleagues.
- *Continue to provide flexibility*: companies can improve job satisfaction and help their employees better balance their work and personal lives by offering employees the flexibility to choose their work hours and location.
- *Foster autonomous work styles*: Organisations can foster a sense of ownership and responsibility in employees by empowering them to make decisions and manage their work independently. This enhanced autonomy can result in greater job performance and job satisfaction.
- *Establish clear channels for communication*: Organisations can implement efficient communication channels and protocols to ensure that the teams remain informed and connected regardless of their work location. In addition, regular check-ins, team meetings, and updates can help prevent feelings of isolation and maintain team cohesion.

- *Develop Remote Training and Development Programs*: Organizations can create online training and development programs, webinars, and workshops to ensure that both in-office and remote workers have the same opportunities for growth and development.
- *Measure Productivity and Performance*: Organizations can implement systems for measuring and monitoring employee work loads, productivity and performance, changing the focus from number of hours worked to outcomes. This approach can help ensure that remote work is effective and beneficial for the organization.
- *Promote a Supportive Culture of Trust*: Organizations must foster a culture of trust by encouraging transparency, open communication, and accountability. Higher job satisfaction and improved performance can result from trusting employees to manage their work effectively.
- *Encourage Feedback*: Organizations can also foster open communication with employees regarding their teleworking experience and the facilities provided by the organization. This feedback can help identify any challenges or areas for improvement, enabling the organization to make necessary adjustments.
- *Address Challenges of Remote Work*: Organizations must acknowledge the potential challenges and distractions of remote work and provide support and guidance for employees in managing these issues, thus helping them maintain their productivity.

6.2.2 IT/IS Implications

The following implications are from an IT/IS perspective:

- *Invest in technology infrastructure*: Organisations can invest in state-of-the-art technology infrastructure, such as secure communication tools, project management software, and collaboration platforms, to ensure seamless interchange between in-office and remote work.

- *Provide Necessary Equipment for Remote Work*: Organisations can supply employees with the essential equipment for remote work, such as laptops, monitors, keyboards, and headsets. Providing the right tools can help employees work efficiently and comfortably from their home office or remote location.
- *Provide Secure Client Devices*: Organisations can provide remote employees with secure devices that have up-to-date security features, such as endpoint protection software and regular security updates. This practice helps ensure that company data is protected, even when accessed from remote locations.
- *Offer Secure Connectivity*: Implementing secure connectivity solutions can help protect sensitive data and maintain the security of business communications. This approach is essential for safeguarding company information and adhering to data protection regulations. Companies should also invest in strong security measures such as multi-factor authentication, firewalls, and encryption to protect their data and systems while employees work remotely.
- *Invest in Collaboration and Communication Tools*: Providing access to reliable communication and collaboration platforms (e.g., video conferencing software, instant messaging, and project management tools) can help remote employees stay connected, share information, and collaborate effectively with their teams.
- *Implement Cloud-Based Solutions*: Cloud-based storage and productivity tools can allow employees to access and work on documents, files, and applications securely from any location, ensuring seamless collaboration and data accessibility.

- *Offer Technical Support*: Establishing a dedicated IT support team or helpdesk for remote employees can help address any technical issues they may encounter, minimizing downtime and ensuring smooth operations.
- *Establish Clear Security Policies:* Develop clear and comprehensive security policies for teleworking employees, outlining expectations, responsibilities, and best practices for securing company data and devices. Communicating these policies helps create a shared understanding of the importance of data security.
- *Provide Security Training:* Offer training and resources on cybersecurity best practices, such as recognizing phishing attempts, creating strong passwords, and securing home Wi-Fi networks. This education can help employees become active participants in maintaining the security of company data.
- *Monitor and Respond to Security Incidents:* Establish a dedicated team or process for monitoring and responding to security incidents, ensuring that any potential threats are quickly identified and addressed.
- *Monitor and Evaluate Teleworking Infrastructure and Security Measures*: Regularly review and assess the effectiveness of the teleworking infrastructure, including equipment, connectivity, and software tools. This process can help identify areas for improvement and ensure that employees have the necessary resources to work effectively from remote locations. Conduct regular security audits and reviews to identify potential vulnerabilities and areas for improvement. This practice helps ensure that the company stays up-to-date with the latest security threats and can adapt its measures accordingly.
- *Plan for Scalability*: As the company grows or the remote workforce expands, plan for the scalability of the teleworking infrastructure to ensure that all employees have access to the necessary tools and resources.

- *Build a "Shared Responsibility" mindset*: While the company is responsible for implementing security measures and providing secure devices, employees also play a crucial role in maintaining security. Encourage a shared responsibility mindset, where both the company and employees work together to protect sensitive data and systems.

6.3 Implications for policy

In this context, the following policy implications can be seen for organisations:

1. <u>Organisational policy for teleworking</u>
    - The organisational policy for teleworking should contain specific details regarding
        - Eligibility and teleworking frequency,
        - Expectations and requirements regarding productivity,
        - Methods of communication,
        - Performance measures and tracking,
        - Exceptions and approvals,
        - Allowed expenditure and claims, and
        - Security requirements.
    - Versions of the policy may be created for management, employees, IT team, human resources, etc., as appropriate.
    - A clear description of possible policy violations to be provided along with methods of dealing with these.
    - Appropriate tools for communication to be identified, customised, and implemented.

- Appropriate productivity applications to be identified, customised, and implemented to track employee progress against deadlines and deliverables.
- Conduct regular sessions to familiarise all stakeholders with the policy and any updates, as appropriate.

2. Organisational policy for VPN usage
   - The organisational policy for VPN usage should contain specific details regarding
     - Connection procedures
     - Compliance
     - Exceptions to policy
     - Applicability
     - Authorised VPN client software
     - Monitoring
     - Inactivity
     - Dealing with violations
   - Conduct regular sessions to familiarise all stakeholders with the policy and any updates, as appropriate.

6.4 Limitations of the study

The research design for the study was a single case study with different units of analysis. In addition, the study utilized a pragmatic, mixed methods approach involving qualitative and quantitative approaches for data collection and analysis. Consequently, the findings from the study cannot be generalized to other organisations.

The qualitative component of the study had a few limitations. First, the researcher single-handedly analysed the interview data. Hence, it was not possible to asses for intrarater reliability and variability. That is, any inconsistency in relating data to the codes (categories, topics, etc.) could not be assessed. This is also due to the nature of the DBA research project which requires the researcher to work independently. Second, saturation was achieved within six interviews which indicates the possibility that the researcher's inexperience with research interviews could have hampered the design of the questions and also the manner in which the additional information was obtained through follow-up questions.

The quantitative component of the study was also limited by the number of participants. The sample size of 200 does not adequately represent the perceptions of the whole organisation. Moreover, since the researcher could not meet with participants to explain the questionnaire or clarify doubts, there could be some errors in understanding which could have impacted the reliability of the captured data.

6.5 Recommendations for Future Research

The overall objective of the study was to offer insights regarding the role of VPN in supporting productivity and security while employees continue to use the option of teleworking in the post-COVID scenario. In this context, a single multi-methods case study was utilised to obtain insights from a single organisation. Future research can extend the study using multiple case studies to compare the status in different organisations.

Additionally, this study utilised a custom questionnaire and two interview schedules to obtain insights from a small sample of participants from a single case organisation, limiting the generalisability of the research outcomes. A future researcher could use a purely quantitative approach with a larger sample to obtain more generalisable outcomes. Moreover, the managers who participated in the study were senior level managers from a limited number of units. A future study could explore the perceptions of multiple managers from the same unit.

Also, the study attempted to combine managerial and technological perspectives with regard to productivity and cybersecurity. Future research could investigate either perspective in deeper detail. Also, the conceptual framework proposed by the study can be tested by a future researcher.

6.6 Conclusion

In the context of the continued desire of employees to telework and the possible resistance to returning full-time to office, this study signifies an attempt to understand factors that can support productivity and cybersecurity. Overall, the study found that the usage of VPN to establish a secure and private connection to the organisation network can support cybersecurity. However, different VPN solutions and the evolving risks and challenges associated with the Internet need to be carefully considered.

Moreover, VPN can support productivity to a certain extent by helping the organisation monitor an employee’s connection to the company network. However, this has to be augmented through the use of productivity applications and organisations have to continue to seek ways and means to engage with employees not merely for work purposes but also to ensure their satisfaction with work and overall well-being.

Regardless of the duration of the existence of telework, it is essential for organisations to continue to explore factors that support their employees’ productivity and welfare. In additon, there has to be a simultaneous endeavour to safeguard the resources entrusted to the organisation by its clients.

APPENDIX A

SURVEY COVER LETTER

Questionnaire for teleworking employees

Dear Respondent,

This questionnaire is part of an empirical research study titled “*VPN Solutions: Balancing Productivity and Security for Business*” as part of my Doctor of Business Administration I attempt to investigate whether productivity and security be achieved in the teleworking scenario in the post-COVID context through the usage of VPN.

I would be grateful if you could contribute to my study by filling up this questionnaire. I assure you that the data collected through this questionnaire shall be kept confidential and will be used only for academic purposes.

Regards,

<<Dr Reji Kurien Thomas>>

<< SSBM>>

APPENDIX B

QUESTIONNAIRE FOR TELEWORKING EMPLOYEES

Section I: Demographic details (Choose only one option for each question)

1. **Age**:

ϒ 21-30 years □ 31-40 years □ 41-50 years □ 51-60 years Other (Please specify) ________________

2. **Gender**:

ϒ Male □ Female

3. Educational Qualification:

ϒ Graduate □ Masters □ Doctorate □ Diploma □ Other (Please specify) ____________________

4. Nature of Employment:

ϒ Full-time □ Part-time □ Contractor □ Intern □ Other (Please specify) ____________________

5. Work Experience in organisation (in years)

ϒ <5 years □ 5 - 10 years □ >10 - 20 years □ >20 – 30 years □ >30 years

Section II: Teleworking experience

The following questions are related to your teleworking experience.

6. Duration of teleworking:

ϒ Only commenced during COVID (i.e., <2 years) □ 2 – 5 years □ >5 years □ Other (Please specify) ________________

7. Were you teleworking before the pandemic?

ϒ Yes □ No

8. Are you continuing to telework after the pandemic?

ϒ Yes □ No

9. If yes, how many days do you telework?

ϒ 1 day a week □ 2 days a week □ 3 days a week □ 4 days a week

10. Who provides the facilities you need to telework?

ϒ My company

ϒ I use facilities purchased by me

ϒ I use a combination of facilities purchased by me/provided by the company

11. Which of these facilities are provided by your company?

ϒ Personal computers (desktop, laptop)

ϒ Mobile devices (smart phones, tablets)

ϒ Remote desktop access

ϒ Secure connectivity

12. How do you feel about the security of your data when teleworking?

ϒ My data are not secure

ϒ My data are somewhat secure

ϒ My data are very secure

13. Who is responsible for the security of your client devices?

ϒ My organisation

ϒ Third-party

ϒ Myself (I use my own devices and am responsible for their security)

ϒ Other (Please specify) _______________

14. Which of the following security measures are implemented/enforced by your organisation? (More than one answer can be chosen)

ϒ Separate user account with limited privileges

ϒ Session locking (access is prevented after a period of inactivity, e.g., 15 minutes)

ϒ Physical securing of telework PCs/laptops (e.g., using cable locks)

ϒ Limited networking capabilities for mobile device

ϒ Antimalware programs

ϒ Personal firewalls

ϒ Regular application of device manufacturer updates and patches to protect devices from known vulnerabilities

ϒ Data encryption of stored data on both built-in storage and removable media

ϒ Data encryption of sensitive data on both built-in storage and removable media

ϒ Requires a password/passcode and/or other authentication before accessing the organization’s resources

ϒ Restrict which applications may be installed through whitelisting or blacklisting

ϒ Use of virtual machines (VMs)

ϒ Backup of data

ϒ Remote access is logged

ϒ Other (Please specify) _______________

15. Overall, do you think you are productive at home than if you had been working in the office?

ϒ Yes □ No

16. Will you consider doing more or less telework than before when things return to ‘normal’?

ϒ Yes, more telework □ Yes, less telework □ No, I want to return to office

17. Which of the following communication channels do you use to communicate with your manager/co-workers?

ϒ E-mail

ϒ Phone (e.g., calls on mobile/land line, WhatsApp call, Skype call)

ϒ Chat/Instant Messaging (e.g., Skype, Microsoft Teams, etc.)

ϒ Video (e.g., Zoom, Microsoft Teams, etc.)

ϒ Other (Please specify) _______________

Section III: Productivity while teleworking

18. The following statements are related to features of your work (Golden and Gajendran, 2019)**. Please indicate your extent to which you agree or disagree with these.**

1: Strongly disagree; 2: Disagree; 3: Neither agree nor disagree; 4: Agree; 5: Strongly Agree

Sl #	**Statement**	**1**	**2**	**3**	**4**	**5**
	Job Role					
1	I am clear what is expected of me at work					
2	I know how to go about getting my job done					
3	I am clear what my duties and responsibilities are					
4	I am clear about the goals and objectives for my department					
5	I understand how my work fits into the overall aim of the organization					
	Job performance					

Sl #	Statement	1	2	3	4	5
6	Overall, I feel I have been effectively fulfilling their roles and responsibilities when teleworking					
7	My overall performance is very good/outstanding when teleworking					
8	My overall performance is good/above average when teleworking*					
9	My overall performance is average when teleworking*					
10	My overall performance is poor/below average when teleworking*					
	Work autonomy					
11	I can make my own decisions about how to schedule my work.					
12	I am allowed to decide on the order in which things are done on the job.					
13	I am allowed to plan how I do my work					
14	I am allowed to use my personal initiative or judgment in carrying out the work					
15	I am allowed to make a lot of decisions on my own					
16	I am given significant autonomy in making decisions					
17	I am allowed to make decisions about what methods I use to complete my work.					
18	I have considerable opportunity for independence and freedom in how I do the work					
19	I am allowed to decide on my own how to go about doing my work					
	Job complexity					
20	My job involves a great deal of task variety					
21	My job requires that I only do one task or activity at a time					
22	My job tasks are intricate and complex					

Sl #	**Statement**	**1**	**2**	**3**	**4**	**5**
28	My job requires me to monitor a great deal of information.					
29	My job requires that I engage in a large amount of thinking.					
30	My job requires me to keep track of more than one thing at a time.					
31	My job requires me to analyse a lot of information.					
32	My job requires the use of a number of skills.					
33	My job is highly specialized in terms of purpose, tasks, or activities.					
34	My job requires very specialized knowledge and skills.					
35	My job requires a depth of knowledge and expertise.					

19. **The following statements are related to your productivity** (Barrero, Bloom and Davis, 2020; ILO, 2020a; Sanhokwe *et al.*, 2022)**. Please indicate your extent to which you agree or disagree with these.**

1: Strongly disagree; 2: Disagree; 3: Neither agree nor disagree; 4: Agree; 5: Strongly Agree

Sl #	**Statement**	**1**	**2**	**3**	**4**	**5**
	Perceived productivity					
1	My productivity at work has improved while teleworking despite greater number of meetings and other communication					
2	I am more efficient in my work when teleworking					
3	I am able to collaborate well with peers while teleworking					
4	I am able to obtain guidance and feedback from my manager while teleworking					
5	I am able to be productive in my work when teleworking					
	Productivity level					

Sl #	**Statement**	**1**	**2**	**3**	**4**	**5**
6	Hugely better - I am 20+% more productive than I expected to be while teleworking					
7	Substantially better - I am to 10% to 19% more productive than I expected to be while teleworking					
8	Better - I am 1% to 9% more productive than I expected to be while teleworking					
9	Same - I am at about the same level of productivity while teleworking					
10	Worse - I am 1% to 9% less productive than I expected to be while teleworking					
11	Substantially worse - I am to 10% to 19% less productive than I expected to be while teleworking					
12	Hugely worse -- I am 20%+ less productive than I expected to be while teleworking					
	Organization measure of Productivity					
13	My organisation sets and communicates clear goals and deadlines in the same way as they do with workers in a physical workspace					
14	My organisation has formed plans to increase my accountability					
15	My organisation analyses important tasks and track progress on a time bound basis					
16	My organisation evaluates quality and quantity instead of time worked					
17	My organisation has shifted metrics from “hours spent” to “tasks accomplished and their quality”					
18	My organisation tracks my achievements					

Section IV: VPN and teleworking

20. Which VPN do you use?

(Please specify)________________________

21. **Why did you choose this VPN?** (Ramesh, Vyas and Ensafi, 2022)

ϒ Actively researching on the Internet e.g., using a search engine

ϒ Recommendations from friends and family

ϒ I randomly encountered them while browsing the web, through advertisements

ϒ Recommendation websites e.g., CNET, TechRadar, Top10vpn

ϒ User review posts e.g., YouTube

ϒ My work provides me a VPN

ϒ Other (Please specify)________________________

22. **What type of subscription do you use?** (Ramesh, Vyas and Ensafi, 2022)

ϒ Free/trial version of a VPN service

ϒ Paid/premium version of a VPN service

ϒ Does not apply (Organisation or Custom VPN)

ϒ Other (Please specify)________________________

23. **Why do you use a VPN product? (Choose all that apply)** (Ramesh, Vyas and Ensafi, 2022)

ϒ To access work networks remotely

ϒ To protect myself from various threats/adversaries

ϒ For file sharing

ϒ To access region-specific content

ϒ Other (Please specify)________________________

24. **How frequently do you use a VPN?** (Ramesh, Vyas and Ensafi, 2022)

ϒ Occasionally

ϒ Every week

ϒ Every day

ϒ All the time/Always on

ϒ Other (Please specify)________________________

25. The following statements are related to the facets of using VPN (Alashi and Aldahawi, 2020; Sharma and Kaur, 2020)**. Please indicate your extent to which you agree or disagree with these.**

1: Strongly disagree; 2: Disagree; 3: Neither agree nor disagree; 4: Agree; 5: Strongly Agree

Sl #	Statement	1	2	3	4	5
	VPN and Productivity					
1	VPN helps with productivity in teleworking					
2	VPN helps secure my connection to the organisation network					
3	I do not have to worry about the security of my data					
	Awareness of VPN Concept					
4	Network that can be connected remotely					
5	Application to encrypt internet connection					
6	Application for digital anonymity					
7	Application for internet censorship circumvention					
8	Tool to secure internet connection					
9	Application for information privacy and security					
	VPN Functioning					
10	VPN is a subscription-based model					
11	VPN uses a high-speed leased line					
12	With VPN, dial-up modems can be used to connect remote locations to the Internet					
	VPN Risks					
13	Hackers and computer thieves can decrypt VPN connection					
14	VPN applications require access rights to sensitive resources such as user accounts					
15	VPN applications contain malware that affects the security of the operating system					
16	VPN applications collect users’ personal information and sell them to external partners					
17	VPN applications track the location of the device by accessing the GPS of the user’s device					
18	VPN applications allow sharing the IP address given by the application with other users					

Sl #	**Statement**	**1**	**2**	**3**	**4**	**5**
19	VPN applications direct the browser to websites without your permission					
20	VPN applications steal network bandwidth and resell it					
	VPN Advantages					
21	VPNs eliminate geographical restrictions					
22	Online privacy is safeguarded					
23	My connection is protected from cybercriminals.					
24	Data transfer is encrypted.					
25	Regional leased lines or even cable networks can be used to connect to the internet.					
26	Cost saving.					
27	Uses public networks to tunnel a private connection					

Thank you very much for your time and effort in participating in this survey!

APPENDIX C

INFORMED CONSENT

Interview Consent Form

Research project title: VPN Solutions: Balancing Productivity and Security For Business

Research investigator: Dr Reji Kurien Thomas

Research Participants name: <<>>

The interview will take approximately 30-45 minutes. We don't anticipate that there are any risks associated with your participation, but you have the right to stop the interview or withdraw from the research at any time.

Thank you for agreeing to be interviewed as part of the above research project. Ethical procedures for academic research require that interviewees explicitly agree to being interviewed and how the information contained in their interview will be used. This consent form is necessary for us to ensure that you understand the purpose of your involvement and that you agree to the conditions of your participation. Would you therefore read the accompanying **information sheet** and then sign this form to certify that you approve the following:

- the interview will be recorded and a transcript will be produced
- you will be sent the transcript and given the opportunity to correct any factual errors

- the transcript of the interview will be analysed by (name of the researcher) as research investigator
- access to the interview transcript will be limited to (name of the researcher) and academic colleagues and researchers with whom he might collaborate as part of the research process
- any summary interview content, or direct quotations from the interview, that are made available through academic publication or other academic outlets will be anonymized so that you cannot be identified, and care will be takento ensure that other information in the interview that could identify yourself is not revealed
- the actual recording will be (kept or destroyed state what will happen) any variation of the conditions above will only occur with your furtherexplicit approval Or a quotation agreement could be incorporated into the interview agreement

Quotation Agreement

I also understand that my words may be quoted directly. With regards to being quoted, please initial next to any of the statements that you agree with:

	I wish to review the notes, transcripts, or other data collected during the research pertaining to my participation.
	I agree to be quoted directly.
	I agree to be quoted directly if my name is not published and a made-up name (pseudonym) is used.
	I agree that the researchers may publish documents that contain quotations by me.

All or part of the content of your interview may be used:

- In academic papers, policy papers or news articles
- On our website and in other media that we may produce such as spoken presentations
- On other feedback events
- In an archive of the project as noted above

By signing this form, I agree that;

1. I am voluntarily taking part in this project. I understand that I don’t have to take part, and I can stop the interview at any time;
2. The transcribed interview or extracts from it may be used as described above;
3. I have read the Information sheet;
4. I don’t expect to receive any benefit or payment for my participation;
5. I can request a copy of the transcript of my interview and may make edits I feel necessary to ensure the effectiveness of any agreement made about confidentiality;
6. I have been able to ask any questions I might have, and I understand that I am free to contact the researcher with any questions I may have in the future.

Printed Name

Participant’s Signature **Date**

Researcher’s Signature **Date**

Contact Information

This research has been reviewed and approved by the University Research Ethics Board. If you have any further questions or concerns about this study, please contact:

Name of researcher: Dr Reji Kurien Thomas

Full address:

Tel:

E-mail:

You can also contact my supervisor:

Name of supervisor:

Full address

Tel:

- E-mail:

What if I have concerns about this research?

If you are worried about this research, or if you are concerned about how it is being conducted, you can contact SSBM by email at contact@ssbm.ch.

APPENDIX D

INTERVIEW GUIDES

IT/IS team interviews

Objectives of the study

The following overarching research question characterises the aims and objectives of the study:

- Can productivity and security be achieved in the teleworking scenario in the post-COVID context through the usage of VPN?

The objectives of the study are as follows:

- To investigate the support provided by VPN usage to achieve productivity and security in the teleworking scenario in the post-COVID context
- To determine the features of the usage of VPN by organisations to support teleworking employees
- To gain insights regarding the risks and benefits of VPN usage in this context
- To identify the facets of a conceptual framework to promote productivity and cybersecurity through VPN usage in organisations which support teleworking

Interview Questions

Thank you for agreeing to take part in this study and to talk to me today, it is much appreciated. I am seeking inputs to understand.

About the person being interviewed (Demographic details)

Please note that you can note down the gender of the person without asking.

1. Please tell me a little bit about yourself. Educational qualification, overall work experience.

2. What is your current role and responsibility at your current organisation?
3. Please describe your organisation: core business, number of employees, number of clients, revenues (range)

About teleworking

4. Did your organisation allow teleworking prior to the pandemic? Were all employees allowed to telework? Do you have any policy or guidelines related to teleworking? Please explain.
5. Please describe the facilities provided by your company to support teleworking employees. For example, client devices e.g., laptops, desktops, smart phones, tablets), network router/extender, client software, etc.
6. Please describe the kind of support provided by the company for teleworking employees. For example, installation assistance, device troubleshooting, etc.

About security

7. What are the main cybersecurity risks and threats that are of concern to your organisation?
8. What are the main cybersecurity challenges faced by your clients?
9. How do you feel about the security of your organisation's/clients' data when employees are teleworking?
10. How do you manage the file and data storage used by the team? What are the different security measures utilised by your organisation? Please describe.

Using VPN in teleworking

11. Which VPN provider does your organisation use?
12. What made you choose this provider rather than other providers? **Please rate the importance of the following criteria while selecting a VPN provider (scale of 1 – 7).** (Ramesh, Vyas and Ensafi, 2022)

Criterion	**Rating (1-7)**
Speed (Quality of service)	
Price of the service	
Easy to understand/use app (GUI)	
Well-documented features	
Ability to change location to access media on websites	

Number of servers located around the world	
Clear explanation of logging and data practices	

13. Please describe the security features of VPN utilised by your organisation.
14. How does your organisation use VPN to support teleworking employees?
15. Are teleworking employees compulsorily asked to use VPN?
16. If yes, are teleworking employees asked to use the same VPN provider or can they choose?
17. What precautions have to be taken at the organisation side if employees can choose their own VPN provider?
18. Please explain how you deal with the situation when employees use their own devices (e.g., laptops, desktops, smart phones, tablets) to telework.
19. How do you feel VPN contributes to the security of your data when employees are teleworking? Which features of VPN are the most useful in this regard?
20. What are the advantages of using VPN in your organisation? Please describe.
21. Correspondingly, what are the risks of using VPN? Please describe.
22. What do you feel are the factors to be considered by the organisation prior to encouraging the use of VPN in the context where employees will continue to telework? Please explain.

Thank you very much for your time and effort in participating in this interview!

Management interviews

Objectives of the study

The following overarching research question characterises the aims and objectives of the study:

- Can productivity and security be achieved in the teleworking scenario in the post-COVID context through the usage of VPN?

The objectives of the study are as follows:

1. To investigate the support provided by VPN usage to achieve productivity and security in the teleworking scenario in the post-COVID context
2. To determine the features of the usage of VPN by organisations to support teleworking employees
3. To gain insights regarding the risks and benefits of VPN usage in this context
4. To identify the facets of a conceptual framework to promote productivity and cybersecurity through VPN usage in organisations which support teleworking

Interview Questions

Thank you for agreeing to take part in this study and to talk to me today, it is much appreciated. I am seeking inputs to understand.

About the person being interviewed (Demographic details)

Please note that you can note down the gender of the person without asking.

1. Please tell me a little bit about yourself. Educational qualification, overall work experience.
2. What is your current role and responsibility at your current organisation?
3. Please describe your organisation: core business, number of employees, number of clients, revenues (range)

About teleworking

4. Did your organisation allow teleworking prior to the pandemic? Were all employees allowed to telework? Do you have any policy or guidelines related to teleworking? Please explain.
5. Do you feel there are certain types of jobs/roles that are more suitable for teleworking?
6. Please describe the facilities provided by your company to support teleworking employees. For example, physical infrastructure for teleworking such as, desk/chair, additional lighting, router/extender, internet connection, telephone connection, etc.
7. Please describe the kind of support you provide to teleworking employees. For example, weekly team meetings, individual discussions, video conferences, etc.
8. What are some of the tools you use for meetings? Example, Google Meet, Zoom, etc.
9. How do you manage the files and data used by the team? Please describe.
10. What are the different security measures utilised by your organisation? Please describe.
11. Please describe the kind of administrative support provided by the company for teleworking employees. For example, reimbursement of internet provider bills, telephone bills, device replacement, infrastructure for teleworking such as, desk/chair, etc.

About Productivity in teleworking

12. Please describe what you understand by the term productivity.
13. How do you feel about the productivity of the employees when teleworking? Does it increase or decrease or remain unchanged? Please explain.
14. What are some of the factors that can influence the productivity of employees? Please describe.
15. How does your organisation use VPN to support teleworking employees? Please describe relevant features.
16. How do you feel VPN contributes to/supports the productivity of the employees when they are teleworking? Please elaborate.
17. In your opinion, what are the advantages of using VPN in your organisation to support teleworking? Please describe.
18. Correspondingly, what are the risks of using VPN? Please describe.

19. What do you feel are the factors to be considered by the organisation prior to encouraging the use of VPN in the context where employees will continue to telework? Please explain.

Thank you very much for your time and effort in participating in this interview!

REFERENCES

Abukari, A. M. and Bankas, E. K. (2020) ‘Some cyber security hygienic protocols for teleworkers in Covid-19 pandemic period and beyond’, *International Journal of Scientific and Engineering Research (IJSER)*, 11(4), pp. 1401–1407. Available at: https://www.ijser.org/onlineResearchPaperViewer.aspx?Some-Cyber-Security-Hygienic-Protocols-For-Teleworkers-In-Covid-19-Pandemic-Period-And-Beyond.pdf.

Adame, D. (2021) *Managing and Securing Endpoints: A Solution for a Telework Environment*. California State University.

Afrianty, T. W., Artatanaya, I. G. L. S. and Burgess, J. (2022) ‘Working from home effectiveness during Covid-19: Evidence from university staff in Indonesia’, *Asia Pacific Management Review*. College of Management, National Cheng Kung University, 27(1), pp. 50–57. doi: 10.1016/j.apmrv.2021.05.002.

Alashi, S. A. and Aldahawi, H. A. (2020) ‘Cybersecurity Management for Virtual Private Network (VPN) Applications: A Proposed Framework for the Governance of their Use in the Kingdom of Saudi Arabia’, *Journal of Information Security and Cybercrimes Research*, 3(1), pp. 31–57. doi: 10.26735/vsdj4585.

Alotaibi, M. N. and Alharbi, Z. H. (2022) ‘Sentiment Analysis to Explore User Perception of Teleworking in Saudi Arabia’, *International Journal of Advanced Computer Science and Applications*, 13(5), pp. 556–563. doi: 10.14569/IJACSA.2022.0130565.

Andriessen, J. H. E. (1991) *Mediated Communication and New Organizational Forms*. Oxford, UK: John Wiley & Sons.

Astroza, S. *et al.* (2020) ‘Mobility Changes, Teleworking, and Remote Communication during the COVID-19 Pandemic in Chile’, *Findings*, 1(Ine 2018), pp. 1–8. doi: 10.32866/001c.13489.

Barker, E. *et al.* (2020) ‘Guide to IPsec VPNs’, *Special Publication (Nist SP) - 800-77r1*, p. 166. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1.pdf%0Ahttp://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-77.pdf.

Barrero, J. M., Bloom, N. and Davis, S. J. (2020) ‘Why Working From Home Will Stick’, *SSRN Electronic Journal*. doi: 10.2139/ssrn.3741644.

Bartlett, M. S. (1950) ‘Tests of significance in factor analysis.’, *British Journal of Psychology*, 3, pp. 77–85.

Baruch, Y. and Nicholson, N. (1997) ‘Home sweet work Requirements for effective’, *Journal of General Management*, 23(2), pp. 15–30.

Bearman, M. (2019) ‘Focus on Methodology: Eliciting rich data: A practical approach to writing semi-structured interview schedules', *Focus on Health Professional Education: A Multi-Professional Journal,* 20(3), pp. 1–11. doi: 10.11157/fohpe.v20i3.387.

Beckel, J. L. O. and Fisher, G. G. (2022) 'Telework and Worker Health and Well-Being: A Review and Recommendations for Research and Practice', *International Journal of Environmental Research and Public Health*, 19(7). doi: 10.3390/ijerph19073879.

Belzunegui-Eraso, A. and Erro-Garcés, A. (2020) 'Teleworking in the context of the Covid-19 crisis', *Sustainability (Switzerland),* 12(9), pp. 1–18. doi: 10.3390/su12093662.

Bentley, T. A. *et al.* (2016) 'The role of organisational support in teleworker wellbeing: A socio-technical systems approach', *Applied Ergonomics*. Elsevier Ltd, 52(January), pp. 207–215. doi: 10.1016/j.apergo.2015.07.019.

Berger, P. and Luckmann, T. (2016) 'The Social Construction of Reality', in *Social Theory Re-Wired*. Second. Routledge, pp. 110–122.

Bhattacharya, S. and Mittal, P. (2020) 'The impact of individual needs on employee performance while teleworking', *Australasian Accounting, Business and Finance Journal*, 14(5), pp. 65–85. doi: 10.14453/aabfj.v14i5.5.

Binkhorst, V. *et al.* (2022) 'Security at the End of the Tunnel : The Anatomy of VPN Mental Models Among Experts and Non-Experts in a Corporate Context', in *31st USENIX Security Symposium*.

Bogdan, R. C. and Biklen, S. K. (2007) *Qualitative research for education: an introduction to theories and methods*.

Boyatzis, R. E. (1998) *Transforming Qualitative Information: Thematic Analysis and Code Development*. Thousand Oaks, CA; London, UK; New Delhi, India: Sage Publications.

Braun, V. and Clarke, V. (2006) 'Using thematic analysis in psychology', *Qualitative Research in Psychology,* 3, pp. 77–101. doi: 10.1057/978-1-137-35913-1.

Brinkmann, S. (2014) 'Unstructured and Semi-structured Interviewing', in Leavy, P. (ed.) *The Oxford Handbook of Qualitative Research*. Oxford University Press, pp. 277–299.

Bryman, A. (2012) *Social Research Methods*. Fourth. Oxford, New York: Oxford University Press. Available at: https://www.ptonline.com/articles/how-to-get-better-mfi-results.

Bucșă, R.-C. (2020) 'Teleworking and Securing Data with VPN Technology', *Economy Transdisciplinarity Cognition*, 23(George Bacovia University), pp. 78–85. Available at: www.ugb.ro/etc.

Burr, V. (2015) *Social Constructionism*. Third. London: Routledge. doi: https://doi.org/10.4324/9781315715421.

Burton, E. *et al.* (2021) 'Delineating the implications of dispersing teams and teleworking in an agile uk construction sector', *Sustainability (Switzerland)*, 13(17), pp. 1–20. doi: 10.3390/su13179981.

Camacho, S. and Barrios, A. (2022) 'Teleworking and technostress: early consequences of a COVID-19 lockdown', *Cognition, Technology and Work*. Springer London, 24(3), pp. 441–457. doi: 10.1007/s10111-022-00693-4.

Campbell, J. and McDonald, C. (2007) 'Defining a conceptual framework for telework research', *ACIS 2007 Proceedings - 18th Australasian Conference on Information Systems*, pp. 813–821.

Carillo, K. *et al.* (2021) 'Adjusting to epidemic-induced telework: empirical insights from teleworkers in France', *European Journal of Information Systems*, 30(1), pp. 69–88. doi: 10.1080/0960085X.2020.1829512.

Carnley, R. and Bagui, S. (2022) 'A Public Infrastructure for a Trusted Wireless World | Enhanced Reader'.

Cerny, B. A. and Kaiser, H. F. (1977) 'A study of a measure of sampling adequacy for factor-analytic correlation matrices', *Multivariate Behavioral Research*, 12(1), pp. 43–47. doi: https://doi.org/10.1207/s15327906mbr1201_3.

CERT-SE (2020) *Security and infrastructure when working from home*. Available at: https://www.cert.se/2020/03/sakerhet-och-infrastruktur-vid-arbete-hemifran (Accessed: 28 November 2022).

Chávez, J. D. (2020) *Key considerations for ensuring the security of organisational data and information in teleworking from home*. niversidadPolitécnica Territorial del estado Aragua, Venezuela. Available at: https://www.researchgate.net/publication/340389338.

Chesley, N. (2014) 'Information and communication technology use, work intensification and employee strain and distress', *Work, Employment and Society*, 28(4), pp. 589–610. doi: 10.1177/0950017013500112.

CISCO (2022) *What Is a VPN? - Virtual Private Network*. Available at: https://www.cisco.com/c/en_in/products/security/vpn-endpoint-security-clients/what-is-vpn.html#~related-topics (Accessed: 21 November 2022).

Cooksey, R. and McDonald, G. (2019) *Surviving and Thriving in Postgraduate Research*. Second. Springer. doi: 10.1007/978-981-13-7747-1_19.

Creswell, J. W. and Plano Clark, V. L. (2018) *Designing and conducting mixed methods research*. Third. SAGE Publications, Inc. doi: 10.1177/1937586719832223.

Creswell, W. J. and Creswell, J. D. (2018) *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. Fifth. Edited by A. J. Mills, G. Durepos, and E. Wiebe. SAGE Publications, Inc. Available at: file:///C:/Users/Harrison/Downloads/John W. Creswell & J. David Creswell - Research Design_ Qualitative, Quantitative, and Mixed Methods Approaches (2018).pdf%0Afile:///C:/Users/Harrison/AppData/Local/Mendeley

Ltd./Mendeley Desktop/Downloaded/Creswell, Cr.

Criscuolo, C. *et al.* (2022) ‘the Role of Telework for Productivity During and Post-Covid-19: Results From an Oecd Survey Among Managers and Workers’, *Oecd Productivity Working Papers*, 1(1), pp. 1–67.

Crowe, S. *et al.* (2011) ‘The case study approach’, *BMC Medical Research Methodology*, 11(100), pp. 1–9.

Cruz, J. E. C. de la, Goyzueta, C. A. R. and Cahuana, C. D. (2020) ‘OpenVProxy: Low Cost Squid Proxy Based Teleworking Environment with OpenVPN Encrypted Tunnels to Provide Confidentiality, Integrity and Availability’, in *2020 IEEE Engineering International Research Conference (EIRCON)*. IEEE, pp. 20–23.

Daniels, K., Lamond, D. and Standen, P. (2001) ‘Teleworking: Frameworks for organizational research’, *Journal of Management Studies*, 38(8), pp. 1151–1185. doi: 10.1111/1467-6486.00276.

Dekkers, R., Carey, L. and Langhorne, P. (2022) *Making Literature Reviews Work: A Multidisciplinary Guide to Systematic Approaches*. Springer International Publishing.

Delanoeije, J. and Verbruggen, M. (2019) ‘The use of work-home practices and work-home conflict: Examining the role of volition and perceived pressure in a multi-method study’, *Frontiers in Psychology*, 10(OCT), pp. 1–18. doi: 10.3389/fpsyg.2019.02362.

Delanoeije, J. and Verbruggen, M. (2020) ‘Between-person and within-person effects of telework: a quasi-field experiment’, *European Journal of Work and Organizational Psychology*. Routledge, 29(6), pp. 795–808. doi: 10.1080/1359432X.2020.1774557.

DeMarrais, K. (2004) ‘Qualitative Interview Studies: Learning Through Experience’, in DeMarrais, K. and Lapan, S. D. (eds) *Foundations for Research: Methods of Inquiry in Education and the Social Sciences*. Mahwah, New Jersey, London: Lawrence Erlbaum Associates, Publishers, pp. 51–68.

Dima, A. M. *et al.* (2019) ‘Sustainable social and individual implications of telework: A new insight into the Romanian labor market’, *Sustainability (Switzerland)*, 11(13). doi: 10.3390/su11133506.

Donnelly, N. and Proctor-Thomson, S. B. (2015) ‘Disrupted work: Home-based teleworking (HbTW) in the aftermath of a natural disaster’, *New Technology, Work and Employment*, 30(1), pp. 47–61. doi: 10.1111/ntwe.12040.

Drumea, C. (2020) ‘Work-related Stress and Subsequent Productivity in a Teleworking Environment Induced by Pandemic-related Confinement. Evidence from the Public’, *Ovidius University Annals, Economic Sciences Series*, XX(1), pp. 337–341. Available at: https://stec.univ-ovidius.ro/html/anale/RO/2020/Section 3/15.pdf.

Ellingson, L. L. (2013) ‘Analysis and Representation Across the Continuum’, in Denzin, N. K. and Lincoln, Y. S. (eds) *Collecting and Interpreting Qualitative Materials*. Fourth.

Los Angeles, London, New Delhi, Singapore, Washington DC: SAGE Publications, Inc., pp. 413–445.

European Trade Union Confederation *et al.* (2002) ‘Framework Agreement on Telework’. Available at: https://www.asi.is/media/312703/teleworking_agreement_en.pdf.

Fana, M. *et al.* (2020) *Telework, work organisation and job quality during the COVID-19 crisis: a qualitative study*. 2020/11. Seville, Spain.

Fitzer, M. M. (1997) ‘Managing From Afar: Performance and Rewards In a Telecommuting Environment’, *Management Compensation*, 29, pp. 65–73.

Garrett, R. K. and Danziger, J. N. (2007) ‘Which telework? Defining and testing a taxonomy of technology-mediated work at a distance’, *Social Science Computer Review*, 25(1), pp. 27–47. doi: 10.1177/0894439306293819.

George, D. and Mallery, P. (2019) *IBM SPSS Statistics 25 Step by Step: A Simple Guide and Reference*. Fifteenth, *IBM SPSS Statistics 25 Step by Step*. Fifteenth. New York, NY; Abingdon, Oxon: Routledge. doi: 10.4324/9781351033909.

Golden, T. D. (2009) ‘Applying technology to work: Toward a better understanding of telework’, *Organisation Management Journal*, 6(4), pp. 241–250. doi: 10.1057/omj.2009.33.

Golden, T. D. and Gajendran, R. S. (2019) ‘Unpacking the Role of a Telecommuter’s Job in Their Performance: Examining Job Complexity, Problem Solving, Interdependence, and Social Support’, *Journal of Business and Psychology*. Journal of Business and Psychology, 34(1), pp. 55–69. doi: 10.1007/s10869-018-9530-4.

Golden, T. D. and Veiga, J. F. (2005) ‘The impact of extent of telecommuting on job satisfaction: Resolving inconsistent findings’, *Journal of Management*, 31(2), pp. 301–318. doi: 10.1177/0149206304271768.

Green, N., Tappin, D. and Bentley, T. (2020) ‘Working From Home Before, During and After the Covid-19 Pandemic: Implications for Workers and Organisations’, *New Zealand Journal of Employment Relations*, 45(2), pp. 5–16. doi: 10.24135/nzjer.v45i2.19.

Greer, T. W. and Payne, S. C. (2014) ‘Overcoming telework challenges: Outcomes of successful telework strategies’, *Psychologist-Manager Journal*, 17(2), pp. 87–111. doi: 10.1037/mgr0000014.

Guetterman, T. C. and Fetters, M. D. (2018) ‘Two Methodological Approaches to the Integration of Mixed Methods and Case Study Designs: A Systematic Review’, *American Behavioral Scientist*, 62(7), pp. 900–918. doi: 10.1177/0002764218772641.

Haines, V. Y., St-Onge, S. and Archambault, M. (2002) ‘Environmental and Person Antecedents of Telecommuting’, *Journal of End User Computing*, 14(3), pp. 32–50.

Harrison, H. *et al.* (2017) ‘Case Study Research: Foundations and Methodological Orientations’, *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, 18(1). Available at: https://www.qualitative-research.net/index.php/fqs/article/download/2655/4079?inline=1%3C/p%3E.

Hercegovac, S., Kernot, J. and Stanley, M. (2020) ‘How Qualitative Case Study Methodology Informs Occupational Therapy Practice: A Scoping Review’, *OTJR Occupation, Participation and Health*, 40(1), pp. 6–16. doi: 10.1177/1539449219850123.

Hoeven, C. L. ter and van Zoonen, W. (2015) ‘Flexible work designs and employee well-being: examining the effects of resources and demands’, *New Technology, Work and Employment*, 30(3), pp. 237–255.

Hyett, N., Kenny, A. and Dickson-Swift, V. (2014) ‘Methodology or method a critical review of qualitative case study reports’, *International Journal of Qualitative Studies on Health and Well-being*, 9(1). doi: 10.3402/qhw.v9.23606.

Hyman, J. and Summers, J. (2004) ‘Lacking balance? Work-life employment practices in the modern economy’, *Personnel Review*, 33(4). doi: 10.1108/00483480410539498.

ILO (2020a) *An employers’ Guide on Working from Home in Response to the Outbreak of COVID-19, International Labour Organization*. Available at: https://www.ilo.org/actemp/publications/WCMS_745024/lang--en/index.htm.

ILO (2020b) *Telework*.

Ionescu, C. A. *et al.* (2022) ‘Sustainability Analysis, Implications, and Effects of the Teleworking System in Romania’, *Sustainability (Switzerland)*, 14(9), pp. 1–18. doi: 10.3390/su14095273.

Irwin, F. (2004) ‘Gaining the air quality and climate benefit for telework’, *World Resources Institute*, (January). Available at: http://pdf.wri.org/teleworkguide.pdf.

Johnson, R. B. and Onwuegbuzie, A. J. (2004) ‘Mixed Methods Research: A Research Paradigm Whose Time Has Come’, *Educational Researcher*, 33(7), pp. 14–26. doi: 10.3102/0013189X033007014.

Kaiser, H. F. (1974) ‘An index of factorial simplicity’, *Psychometrika*, 39, pp. 31–36. doi: https://doi.org/10.1007/BF02291575.

Kazekami, S. (2020) ‘Mechanisms to improve labor productivity by performing telework’, *Telecommunications Policy*. Elsevier Ltd, 44(2), p. 101868. doi: 10.1016/j.telpol.2019.101868.

Kelliher, C. and Anderson, D. (2010) ‘Doing more with less? Flexible working practices and the intensification of work’, *Human Relations*, 63(1), pp. 83–106.

Kerrin, M. and Hone, K. (2001) ‘Job seekers’ perceptions of teleworking: A cognitive mapping approach’, *New Technology, Work and Employment*, 16(2), pp. 130–143. doi:

10.1111/1468-005X.00082.

Khan, M. T. *et al.* (2018) ‘An empirical analysis of the commercial VPN ecosystem’, *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, pp. 443–456. doi: 10.1145/3278532.3278570.

Kitchenham, A. D. (2010) ‘Mixed Methods in Case Study Research’, in Mills, A. J., Durepos, G., and Wiebe, E. (eds) *Encyclopedia of Case Study Research*. SAGE Publications, Inc., pp. 561–564.

Korty, A., Calarco, D. and Spencer, M. (2021) ‘Balancing risk with virtual private networking during a pandemic’, *Business Horizons*, 64(6), pp. 757–761. doi: 10.1016/j.bushor.2021.07.011.

Kossek, E. E., Lautsch, B. A. and Eaton, S. C. (2009) ‘“Good Teleworking”: Under What Conditions Does Teleworking Enhance Employees’ Well-being?’, in Amichai-Hamburger, Y. (ed.) *Technology and Psychological Well-being*. Cambridge, UK: Cambridge University Press, pp. 148–173. doi: 10.1017/CBO9780511635373.

Kossek, E. E., Thompson, R. J. and Lautsch, B. A. (2015) ‘Balanced workplace flexibility: Avoiding the traps’, *California Management Review*, 57(4), pp. 5–25. doi: 10.1525/cmr.2015.57.4.5.

Larsen, T. P. and Andersen, S. K. (2007) ‘A new mode of European regulation? The implementation of the autonomous framework agreement on telework in five countries’, *European Journal of Industrial Relations*, 13(2), pp. 181–198. doi: 10.1177/0959680107078252.

Lewis, J. and Nicholls, C. M. (2014) ‘Design Issues’, in Nicholls, C. M. et al. (eds) *Qualitative Research Practice: A Guide for Social Science Students and Researchers*. Second. Thousand Oaks, CA: SAGE Publications, Inc.

van Lier, T., De Witte, A. and Macharis, C. (2012) ‘The Impact of Telework on Transport Externalities: The Case of Brussels Capital Region’, *Procedia - Social and Behavioral Sciences*, 54(0), pp. 240–250. doi: 10.1016/j.sbspro.2012.09.743.

Loia, F. and Adinolfi, P. (2021) ‘Teleworking as an eco-innovation for sustainable development: Assessing collective perceptions during COVID-19’, *Sustainability (Switzerland)*, 13(9), pp. 1–16. doi: 10.3390/su13094823.

Mahler, J. (2012) ‘The Telework Divide: Managerial and Personnel Challenges of Telework’, *Review of Public Personnel Administration*, 32(4), pp. 407–418. doi: 10.1177/0734371X12458127.

Mannebäck, E. and Padyab, A. (2021) ‘Challenges of Managing Information Security during the Pandemic’, *Challenges*, 12(2), p. 30. doi: 10.3390/challe12020030.

Manser, K. *et al.* (2004) *Austin’s Pilot Telework Program to Impact Air Quality and Reduce Traffic Congestion: Summary of our Citywide Telework Pilot Program*. Austin, Texas.

Maréchal, G. (2010) ‘Constructivism’, in *Encyclopedia of Case Study Research*, pp. 220–225.

Marshall, C. and Rossman, G. B. (2016) *Designing Qualitative Research*. Thousand Oaks, CA: SAGE Publications, Inc.

McClelland, D. (1965) ‘Toward a Theory of Motive Acquisition.’, *American Psychologistsychologist*, 20, pp. 321–333. doi: 10.1037/h0022225.

McClelland, D. (1976) *The Achieving Society*. New York: Irvington.

McDonald, A. *et al.* (2018) ‘403 Forbidden: A global view of CDN geoblocking’, *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, pp. 218–230. doi: 10.1145/3278532.3278552.

Meneses, F. *et al.* (2020) ‘An integration of slicing, NFV, and SDN for mobility management in corporate environments’, *Transactions on Emerging Telecommunications Technologies*, 31(1), pp. 1–18. doi: 10.1002/ett.3615.

Merriam, S. B. and Tisdell, E. J. (2016) *Qualitative research: A guide to design and implementation*. Fourth. San Francisco, CA: Jossey-Bass.

Mihalca, L., Irimias, T. and Brendea, G. (2021) ‘Teleworking During The Covid-19 Pandemic: Determining Factors Of Perceived Work Productivity, Job Performance, And Satisfaction’, *Amfiteatru Economic*, 23(58), pp. 620–636. doi: 10.24818/EA/2021/58/620.

Mills, A. J., Durepos, G. and Wiebe, E. (eds) (2010) *Encyclopedia of Case Study Research*. SAGE Publications, Inc.

Mılası, S., González-Vázquez, I. and Fernández-Macías, E. (2021) *Telework Before the Covid-19 Pandemic: Trends and Drivers of Differences Across the Eu*. 21. Available at: https://www.oecd-ilibrary.org/economics/telework-before-the-covid-19-pandemic_d5e42dd1-en.

Molina, M. D., Shyam Sundar, S. and Gambino, A. (2019) ‘Online privacy in public places: How do location, terms and conditions and VPN influence disclosure?’, *Conference on Human Factors in Computing Systems - Proceedings*, pp. 1–6. doi: 10.1145/3290607.3312932.

Morganson, V. J. *et al.* (2010) ‘Comparing telework locations and traditional work arrangements: Differences in work-life balance support, job satisfaction, and inclusion’, *Journal of Managerial Psychology*, 25(6), pp. 578–595. doi: 10.1108/02683941011056941.

MSB (2020a) ‘Informationssäkerhet för dig som arbetar hemma’. MSB.

MSB (2020b) ‘Till dig som samordnar organisationens informationssäkerhet när flera arbetar på distans’. MSB.

Nelson, D. L. (1990) ‘Individual Adjustment to Information-Driven Technologies: A Critical Review’, *MIS Quarterly*, 14(1), pp. 79–98.

Nemteanu, M. S., Dabija, D. C. and Stanca, L. (2021) ‘The Influence Of Teleworking On Performance And Employees’ Counterproductive Behaviour’, *Amfiteatru Economic*, 23(58), pp. 601–619. doi: 10.24818/EA/2021/58/601.

Newell, R. and Burnard, P. (2011) *Research for Evidence-Based Practice in Healthcare*. Second. Wiley.

Nilles, J. M. (1997) ‘Telework: Enabling distributed organizations: Implications for it managers’, *Information Systems Management*, 14(4), pp. 7–14. doi: 10.1080/10580539708907069.

NIST (2016) ‘Guide to Enterprise Telework, Own Device (BYOD) Security’, *NIST Special Publication 800-46*. National Institute of Standards and Technology. Available at: http://dx.doi.org/10.6028/NIST.SP.800-46r2.

NIST (no date) *virtual private network (VPN)*. Available at: https://csrc.nist.gov/glossary/term/virtual_private_network (Accessed: 28 November 2022).

Nobori, D. and Shinjo, Y. (2014) ‘VPN Gate: A volunteer-organized public VPN relay system with blocking resistance for bypassing government censorship firewalls’, *Proceedings of the 11th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2014*, pp. 229–241.

OECD (2020) ‘Productivity gains from teleworking in the post COVID-19 era: How can public policies make it happen?’, *OECD Policy Responses to Coronavirus (COVID-19)*, (September), pp. 1–24. Available at: https://read.oecd-ilibrary.org/view/?ref=135_135250-u15liwp4jd&title=Productivity-gains-from-teleworking-in-the-post-COVID-19-era.

Olson, M. H. (1981) *Office Work In The Home: Scenarios and Prospects for the 1990’s*. New York: Diebold Group.

Olson, M. H. (1983) ‘Remote office work: Changing work patterns in space and time’, *Communications of the ACM*, 26(3), pp. 182–187. doi: 10.1145/358061.358068.

Patton, M. (2015) *Qualitative research & evaluation methods: Integrating theory and practice : The definitive text of qualitative inquiry frameworks and options*. 4th edn. Thousand Oaks, CA: Sage.

Powell, C. R. (2021) *The Impact of Telework on Organizational Cybersecurity During the COVID-19 Pandemic*. Utica College.

Prosser, T. (2011) ‘The implementation of the telework and work-related stress agreements: European social dialogue through “soft” law?’, *European Journal of Industrial Relations*, 17(3), pp. 245–260. doi: 10.1177/0959680111410964.

Proudfoot, K. (2022) ‘Inductive/Deductive Hybrid Thematic Analysis in Mixed Methods Research’, *Journal of Mixed Methods Research*, 0(0), pp. 1–19. doi: 10.1177/15586898221126816.

Pyöriä, P. (2011) ‘Managing telework: Risks, fears and rules’, *Management Research Review*, 34(4), pp. 386–399. doi: 10.1108/01409171111117843.

Qu, S. Q. and Dumay, J. (2011) ‘The qualitative research interview’, *Qualitative Research in Accounting and Management*, 8(3), pp. 238–264. doi: 10.1108/11766091111162070.

Ramesh, R., Vyas, A. and Ensafi, R. (2022) ‘“All of them claim to be the best”: Multi-perspective study of VPN users and VPN providers’. Available at: http://arxiv.org/abs/2208.03505.

Richards, L. and Morse, J. M. (2013) *Readme first for a users’ guide to qualitative methods*. Third. Los Angeles, London, New Delhi, Singapore, Washington DC: SAGE Publications, Inc.

Rose, S. *et al.* (2020) *Zero Trust Architecture*, *NIST Special Publication 800-207*. doi: 10.1201/9781003189664-11.

Sanhokwe, H. *et al.* (2022) ‘Impact of COVID-19 Induced Teleworking Arrangements on Employees in NGOs: Implications for Policy and Practice for Leadership’, *SAGE Open*, 12(2). doi: 10.1177/21582440221079908.

Saunders, M., Lewis, P. and Thornhill, A. (2019) *Research Methods for Business Students*. Eighth. Harlow, UK: Pearson Education Limited. Available at: https://www.amazon.com/Research-Methods-for-Business-Students/dp/1292208783/ref=sr_1_2?dchild=1&qid=1614706531&refinements=p_27%3AAdrian+Thornhill+%2F+Philip+Lewis+%2F+Mark+N.+K.+Saunders&s=books&sr=1-2&text=Adrian+Thornhill+%2F+Philip+Lewis+%2F+Mark+N.+K.

Scarfone, K., Greene, J. and Souppaya, M. (2020) *Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) solutions*, *ITL Bulletin*. Information Technology Laboratory. Available at: https://csrc.nist.gov/publications/detail/itl-bulletin/2020/03/security-for-enterprise-telework-remote-access-and-byod/final (Accessed: 4 August 2022).

Seal, W. (2012) ‘Some proposals for impactful management control research’, *Qualitative Research in Accounting and Management*, 9(3), pp. 228–244. doi: 10.1108/11766091211257461.

Shardeshmukh, S. R., Sharma, D. and Golden, T. (2012) ‘Impact of telework on exhaustion and job engagement: a job demands and job resources model Telework: Out comes and Facilitators for Employees’, *New Technology, Work and Employment*, 27(3), pp. 193–207.

Sharma, D. Y. K. and Kaur, C. (2020) ‘The Vital Role of Virtual Private Network (VPN) in Making Secure Connection Over Internet World’, *International Journal of Recent Technology and Engineering (IJRTE)*, 8(6), pp. 2336–2339. doi: 10.35940/ijrte.f8335.038620.

Siha, S. M. and Monroe, R. W. (2006) ‘Telecommuting’s past and future: A literature review and research agenda’, *Business Process Management Journal*, 12(4), pp. 455–482. doi: 10.1108/14637150610678078.

Song, Y. and Gao, J. (2018) *Does Telework Stress Employees Out? A Study on Working at Home and Subjective Well-Being for Wage/Salary Workers*. 11993. Bonn, Germany. doi: 10.1007/s10902-019-00196-6.

Stake, R. E. (2013) *Multiple Case Study Analysis*. New York, London: The Guilford Press.

Stern, E. and Holti, R. (1986) *Distance Working Study: Conclusions and Recommendations for Action*. Brussels: Directorate-General for Science, Research and Development, Commission of the European Communities.

Teddlie, C. and Tashakkori, A. (2009) *Foundations of Mixed Methods Research*. SAGE Publications, Inc.

Teddlie, C. and Yu, F. (2007) ‘Mixed Methods Sampling’, *Journal of Mixed Methods Research*, 1(1), pp. 77–100. doi: 10.1177/1558689806292430.

Tietze, S. and Musson, G. (2004) ‘RECASTING THE HOME-WORK RELATIONSHIP: A CASE OF MUTUAL ADJUSTMENT?’, *Organization Studies*, 30(3), pp. 1–40.

Tokarchuk, O., Gabriele, R. and Neglia, G. (2021) ‘Teleworking during the COVID-19 crisis in Italy: Evidence and tentative interpretations’, *Sustainability (Switzerland)*, 13(4), pp. 1–12. doi: 10.3390/su13042147.

Turner, C., Turner, C. B. and Shen, Y. (2020) ‘Cybersecurity Concerns & Teleworking in the COVID-19 Era: A Socio-Cybersecurity Analysis of Organizational Behavior’, *Journal of Advanced Research in Social Sciences*, 3(2), pp. 22–30. doi: 10.33422/jarss.v3i2.502.

Ursery, S. (2003) ‘Austin fights air pollution with telework program’, *American City & County*. Available at: https://www.americancityandcounty.com/2003/05/01/technology-austin-fights-air-pollution-with-telework-program/.

de Vries, H., Tummers, L. and Bekkers, V. (2019) ‘The Benefits of Teleworking in the Public Sector: Reality or Rhetoric?’, *Review of Public Personnel Administration*, 39(4), pp. 570–593. doi: 10.1177/0734371X18760124.

Wang, Z. *et al.* (2017) ‘Your state is not mine: A closer look at evading stateful internet censorship’, *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, Part F1319, pp. 114–127. doi: 10.1145/3131365.3131374.

Ward, K. and Street, C. (2010) ‘Reliability’, in Mills, A. J., Durepos, G., and Wiebe, E. (eds) *Encyclopedia of Case Study Research*. SAGE Publications, Inc., pp. 800–802.

Weber, C. *et al.* (2022) ‘Future Teleworking Inclinations Post-COVID-19: Examining the Role of Teleworking Conditions and Perceived Productivity’, *Frontiers in Psychology*, 13(May), pp. 1–17. doi: 10.3389/fpsyg.2022.863197.

Weinert, C. *et al.* (2014) ‘Does teleworking negatively influence IT professionals? An empirical analysis of IT personnel’s telework-enabled stress’, *SIGMIS-CPR 2014 - Proceedings of the 2014 Conference on Computers and People Research*, pp. 139–147. doi: 10.1145/2599990.2600011.

Yin, R. K. (2014) *Case Study Research: Design and Methods*. Fifth. Los Angeles, London, New Delhi, Singapore, Washington DC: Sage.

Yin, R. K. (2018) *Case study research and applications: Design and methods*. doi: 10.1177/109634809702100108.