AFRICAN JOURNAL IN EDUCATION AND TRANSFORMATION
Volume 1, Edition No 1 Special Edition, February 2021

Investigating Employee Performance & Minimization of Staff Operational Risks during Telecommuting In A Company At Midrand, Johannesburg.

Ineshree Naidoo; Reginald Legoabe
Email: ineshree@gmail.com

Abstract: COVID 19 has necessitated the need for employees and employers to evaluate their readiness and flexibility to crisis management in the 4th industrial revolution era. The pandemic has illustrated how capital intensive and digitized, the working environment may need to be. This has therefore raised questions and concerns around the human resource capacity of the South African institutions and the labour force's competency to function in a digital economy. This study investigated the impact that exclusive telecommuting had on employee performance and also focused on measures that the company implemented to mitigate their operational risks. This topic was elected based on the current COVID19 global pandemic which has had an impact on international trade, social as well as economic conditions. Companies have been catapulted into an exclusive telecommuting working environment as opposed to the traditional office environment. This study aimed to bridge the gap in the literature especially with regards to a South African context however it would be applicable at an international level as well. The research was qualitative and used a thematic analysis of data which consisted of interviews conducted with Respondents. The results from the research indicate that employee performance has been enhanced while telecommuting and that the company has risk mitigation elements in effect but there is an opportunity for advancement of such risk factors. This paper looks at the challenges that several organisations have encountered during the pandemic regarding skills utilisation in managing and preventing the COVID 19 crisis in different areas of service delivery and how both employers as well as employees have had to cope with remote working strategies.

Keywords : *COVID 19, 4th Industrial Revolution, digital economy, Remote Work Strategies*

Introduction

Throughout the twenty-first (21st) century, technological advancements have improved many aspects of daily interactions, especially the ability to augment communication in a traditional workplace environment.

Telecommuting implies the ability to work remotely from anywhere including the home space and has drastically transformed the corporate sectors traditional office hours. Telecommuting has allowed employees the flexibility to work from another setting, excluding the office. The onset of a global pandemic, COVID-19 has exacerbated the need for employees to exclusively telecommute as a result of strict lockdown restrictions imposed by the South African government.

The impact is that employers have to maintain communication and ensure their effectiveness using a virtual platform while employees have to ensure the privacy of client data as well as avert threats posed by operational risks.

The study aims to address the gap in the literature and contribute towards understanding how companies and employees are striving to remain effective in executing their functions under the strict regulatory conditions imposed by COVID-19.

The study has contextual validity and would also appeal to the domestic and international communities as this is currently a global matter that is affecting everyone.

With the onset of the global COVID-19 pandemic, many businesses have been forced to implement stringent working measures to minimise exposure of the virus to its employees. The company is a digital solutions company that uses single, multi and omnichannel approaches to heighten its customers' virtual experience.

The company offers clients the ability to introduce a fully digital system by building applications and platforms that will enable the clients to achieve quicker results within their respective domains.

The company also provides its clientele data storage solutions such as cloud management, data integration and database administration. Further to these services, the company offers ideation workshops and design thinking, coupled with providing advice to companies on the preferred software solutions to digitise and organise their business needs.

The company has a high demand for elite customer interaction that is focused on designing a tailor-made digital resolution to customer challenges. The organisation is currently faced with restricting its employees and clients, face-to-face contact and had to implement other measures to ensure that work takes place outside the traditional office setting.

This has culminated in the creation of a virtual working environment for employees. Ugargol and Patrick (2018:41) state that the global and traditional nature of the workforce environment is changing and companies need to adapt. The authors further reiterate that a flexible working environment, which includes the option to work remotely, will result in employees that are committed, loyal and improve employee performance.

The company is faced with the challenge of being able to provide services to all clientele while ensuring that workplace connectivity and communication takes place. Further to this, the company has to handle issues such as client privacy and ensure that operational risks are minimised.

Perrera, Kerr and Kimura (2014:3) highlight that operational risks arise when there is inadequate attention to processes and systems, and this has the potential to result in a financial loss for the company and threaten other areas of company functionality.

Having employees with access to confidential data whilst working from home could also pose a further challenge, and the research is aimed at assessing if a virtual work environment can be implemented whilst ensuring that there is a harmonious integration with company rules and standard workplace practices.

Research Problem

The current research problem is that the COVID-19 pandemic has resulted in company employees working exclusively from virtual offices at home with a lack of access to the standard system security protocols and control mechanisms customarily found in the workplace.

Whilst telecommuting, employees will have access to confidential data relating to the client and their businesses and now have the added burden of ensuring the privacy of such information.

Further to this, the problem is that a virtual working environment contributes towards the increase in operational risks, such as non-compliance with internal procedures, system irregularities and cyber threats.

The problem to be investigated relates to how employees' can meet their expected work standards and how they minimise operational risks whilst working from home.

The study will also seek to examine how the company mitigates the risks emanating from telecommuting with a focus on operational threats. These operational threats have the potential to threaten the daily functional business processes. The independent variable is telecommuting, and the dependent variable identified is operational risks.

Aim of Study

The aim of the study is to investigate the impact that exclusive telecommuting has on employee performance and to focus on measures that the company implemented to mitigate their operational risks in the context of employee telecommuting during the COVID-19 pandemic.

A phenomenological research study is conducted to ascertain different employees individual experiences in achieving their work objectives, performance indicators, as well as any operational risks that they encounter based on the various types of work conducted. Recommendations will be put forth to the company based on the findings of the study to strengthen organisational performance under similar conditions.

Research Objectives

The study seeks to achieve the following objectives:-

- **To establish if telecommuting during COVID-19 allows employees to achieve individual expected performance standards of the company.**
- **To ascertain what measures the company has implemented to mitigate operational risks.**
- **To establish how the company can increase or realign mitigation factors to further minimise operational risk.**
- **To advise on how employee performance can be enhanced while telecommuting during COVID-19.**

Research Questions

The study seeks to answer the folling research questions:-

- **Does telecommuting during COVID-19 allow employees to attain individual expected performance standards of the company**
- **What measures does the company implement to mitigate operational risks?**
- **What mitigation factors can the company implement to minimise operational risks?**
- **How can employee performance be enhanced in a virtual working environment during the COVID-19 pandemic?**

Significance of Study

The findings of this study will contribute towards the gap in the literature, which seeks to identify how COVID-19 has impacted employees as employees were forced from a traditional office environment to a virtual office settings.

The global pandemic has had a significant impact on economies around the world, and companies have been thrust into an unprecedented working dynamic that most have never explored before.

It is thus of great importance for domestic and international companies to assess if their employees can function at optimal standards and achieve their expected performance outcomes whilst telecommuting, primarily through the COVID-19 pandemic. This will enable more clearer understanding of how telecommuting has impacted on employee performance as well as the ability to assess how proactive employers have been in alleviating foreseeable operational risks arising out of telecommuting.

Studies on telecommuting and employee performance are extensive, however, there is paucity on the impact that COVID-19 and the effect of extended telecommuting work experience on employee attainment of expected performance standards.

Literature Review

Since March 2020, South Africans have been afflicted by the COVID-19 pandemic. Alon, Doepke & Olmstead-Rumsey (2020:2) states that besides the impact on health, the pandemic will also lead to a major global economic downturn. This has impacted on how companies strategise and aim to continue working from the confines of their home.

Telecommuting, according to Jackson and Fransman (2018:2), is the ability to work from home. According to Jackson and Fransman (2018:2), this can have a positive impact on employee productivity and job satisfaction.

The company, a digital solutions company, has restructured their working environment from the traditional office space to a virtual working atmosphere. This has resulted in all employees those who are technical and non-technical being required to interface with clients from home and maintain communication at the client and employer level.

The study aims to determine if telecommuting has impacted on the employees' performance in terms of reaching their expected standards and if there is adequate mitigation of operational risks by the company.

Although the notion of telecommuting is not a new phenomenon, many companies were content in a traditional office setting. This chapter highlights the regulations and legislation which govern the area of COVID 19 and how this has resulted in many companies transitioning to a completely virtual arena.

In addition to this, the impact that telecommuting has on employees will be assessed as well as the operational risks that emanate when employees work outside the confines of the office space.

According to the World Health Organisation (WHO), COVID 19 is a global health pandemic which is spreading rapidly and causing fatalities across the world. Countries such as Spain, the UK and the United States of America (USA) have been greatly affected according to Sekyere, Bohler-Muller and Hongoro (2020:1) despite having an advanced health care system.

The authors further suggest that this pandemic could have a crippling effect on the already strained weak health systems of African countries. The South African government has initiated stringent measures to reduce the curve of COVID 19 infections and allow the government time to adequately supplement the health sector.

As a response to the outbreak of COVID 19 in SA, Sekyere, Bohler-Muller and Hongoro (2020:2) state that President Cyril Ramaphosa together with an appointed National Command Council declared a national state of disaster and an initial twenty-one (21) day lockdown period was instituted.

The authors further reiterate that this allowed for different structures to be implemented and an array of regulations to be developed. These regulations had an immediate impact on the movement of people during the restrictive lockdown period. Only people who fall under the ambit of essential services were able to physically go to work, and all other businesses, including restaurants and take-away places, had to temporarily close their doors. This had

Sekyere, Bohler-Muller and Hongoro (2020:3) highlight that the regulations implemented required all non-essential workers to stay at home unless they required medical care or needed groceries. In addition to this, the authors highlight the social distancing policy, which led to the pause of social and religious gatherings as well as schooling.

These measures have had many challenges for large numbers of people and companies have had to become creative to try and maintain and generate their revenue while allowing employees to continue to work from home. While this is not possible for all businesses such as restaurants, companies in areas such as Information Communication Technology (ICT) finance and telecommunications were able to rise to the challenge.

According to Krugel and Viljoen (2020:3), several South African companies will be adversely impacted by COVID 19, and this includes sectors such as automotive manufacturers, retail and hospitality. The companies who would remain minimally affected are those whose business platforms are sustainable via a virtual platform and the authors suggest that COVID 19 induced business interruptions would have a ripple effect on other sectors

The impact of the regulations is vast and varied and include economic and social disruptions. Businesses who are unable to operate using a virtual platform might have to close permanently while other businesses are striving to enhance their business platforms in other ways.

According to Krugel and Viljoen (2020:3), businesses need to have a clearly defined plan to handle the COVID 19 crisis and ensure their viability within a South African context.

Krugel and Viljoen (2020: 3) suggest that while the regulations have had a major impact on health and socio-economic conditions, companies should re-strategise and explore alternative options that would position their businesses for success.

One such option would be to strive for an exclusive telecommuting environment which allows traditional business processes to occur from home. This would ensure that people can work from the confines of their home while not risking exposure to COVID 19.

Understanding Telecommuting

Author Schall (2019:14) states that telecommuting is the ability to use telecommunication technologies which allows employees to perform their duties remotely and not within the boundaries of a traditional office setting. The author further highlights that since the 1900s telecommuting has gained momentum as a business practice which allows companies to reduce costs associated with operating a physical business premise.

While telecommuting remained a choice between employer and employee, with the onset of the COVID 19 pandemic many companies have been forced to resort to an exclusive telecommuting working environment.

Telecommuting, according to Allen, Golden and Shockley (2015:42) is referred to as remote work, flexible work and even distance work. While different terms are used, essential elements are allowing an employee to conduct work activities from a location outside of the physical office.

Characteristics of Telecommuting

For telecommuting to succeed Angeles (2019) states that merely providing an internet connection and a computer to employees would not suffice. The author highlights that the following characteristics for the successful implementation of telecommuting should be considered. Allen, Golden and Shockley (2015) and authors Belzunegui-Eraso and Erro-Garces (2020) link the following success factors with effective telecommuting.

- Eligibility: Selection Criteria and Requirements
- Technological Infrastructure Support
- Remote Worker Management & Performance Evaluations
- Telecommuting Rules and Policies
- Telecommuter Agreement and Contract

Eligibility

Eligibility, according to Linden and Oljemark (2018:43) refers to the ability of the employee to work in an environment isolated from co-workers and still be able to meet clearly defined outcomes. This implies there must be due consideration for personal factors, professionalism and dependability. An employee would be an ideal candidate for telecommuting if they are a team player and dependable, coupled with a high degree of professionalism.

In addition to this Allen, Golden and Shockley (2015:51) posit that an employee will excel at telecommuting if they have a proven record of being dependable such as responding on time to emails and having completed prior projects with ease and without constant supervision.

Despite the present situation whereby all employees are required to telecommute to prevent the spread of COVID 19, and due to government-imposed regulations, companies can measure their accomplishments based on these factors.

Technological Infrastructure Support.

Technological infrastructure support implies that the technological elements must be in place to ensure that there is optimal support provided to the employee (Belzunegui-Eraso and Erro-Garces, 2020:4-5)

The major accessibility points to enhance the support provided to employees according to Richard (2012:24) is having access to a high-speed WIFI network, a network which minimises risk and the proper anti-virus software to ensure the integrity of the access.

Remote Employee Performance Evaluation

Other aspects of telecommuting as reiterated by Schall (2019:8-10) is for the employer to ensure that there are performance evaluations which address the unique aspects of telecommuting. In addition Allen, Golden and Shockley (2015:53-54) emphasize that the employer must have clearly defined rules and policies which specify the parameters for employees whilst telecommuting. In addition to this, there should also be a detailed agreement and contract which addresses the distinctive features of telecommuting.

Companies that have been forced by regulations to institute telecommuting might not have had these policies and technical infrastructure place, which means that additional difficulties might be experienced whilst trying to telecommute.

This could also change the telecommuting experience for the employee as if there is a lack of support and infrastructure, it might pose an impediment to employees achieving their expected performance standards.

This has the potential to stifle the performance of employees who are traditionally exceptional employees. The unique aspects of telecommuting make certain aspects challenging for the employee to reach their regular performance standards.

According to Allen, Golden and Shockley (2015:49), a variety of employee roles can be fulfilled more productively while having a telecommuting agreement in place. Some of the reasons offered is that positions that requires a high degree of reading, writing and an in-depth level of concentration, might be easier achieved within the confines of a telecommuting environment with minimum distractions.

Some of the primary reasons provided by Allen, Golden and Shockley (2015:55) is the ability to take services to the client's doorstep thereby allowing the employee to meet performance standards and improve the quality of work iutputs.

The study conducted by Allen, Golden and Shockley (2015:56) indicate that a telecommuting arrangement has a positive relationship with an enhanced quality of work from the employee.

Advantages of Telecommuting

Having a virtual working environment has its advantages as this offers a virtual team the opportunity to collaborate across the globe on projects.

This allows companies to be flexible in a variety of aspects related to their business processes. Bhat, Pande and Ahuja (2017:34) state that companies can bring the right people together at the right time for the execution of responsibilities.

The authors also suggest that a virtual office space allows a company to create workplace flexibility which is directly related to job satisfaction for many employees. The effectiveness of virtual teams and work has a direct impact on employee satisfaction and can result in employees achieving and even exceeding expected standards.

During COVID-19 lockdown, the South African government instituted strict regulations which restrict movement, so companies had to plan and develop new methods to communicate with employees and their clients.

Deciding to work solely from a virtual office was imposed on companies, (Lewis, 2020:2), as a means to implement social distancing measures and control the spread of the COVID-19 virus. According to Lewis (2020:2) employers had to review their existing resources and confirm if their IT infrastructure could support remote work.

From the literature, it is evident that a virtual office environment has many considerations and that employers have to ensure that employees are equipped with the necessary hardware and software to perform their duties.

Garg and van der Rijst (2015:34) posit that a uniquely South African perspective highlights evidence to show that a flexible or virtual working space allows employees to have increased levels of productivity. The authors submit that employees benefit from this situation as there is less time spent travelling and more flexibility at home.

Garg and van der Rijst (2015:38) reiterate that telecommuting has a positive impact on employees and results in employees being able to adjust their specific jobs to suit the virtual work environment with ease.

Further to this, the authors indicate that empirical studies suggest that employees that telecommute experienced positive outcomes relating to an improved work-life balance and higher productivity levels. The authors support the notion that telecommuting contributes positively to increased productivity levels.

Onyemaechi, Chinyere and Emmanuel (2018:56) agree that telecommuting has a positive impact on employees workplace productivity. The authors posit that telecommuting allows for large scale flexibility and the more efficient use of a company's information systems, at any given time. The other major impact as reiterated by Onyemaechi, Chinyere and Emmanuel (2018:56) is the change of focus of employees from just merely being present at work to a clearer focus on achieving the expected results.

The individual workers in the organisation receive a major impact on the adoption of telecommuting. These individuals telecommute and hence receive the direct impact from telecommuting practices. These impacts are positive and sometimes negative to the individuals.

One positive impact of telecommuting on individual workers is that they do not commute back and forth to work and hence can cut down on transportation cost (Hunton, 2005). Concerning cutting down on cost, the individual workers are therefore able to have an improved balance between their work and life at home. Improved job satisfaction leads to highly motivated workers when telecommuting is adopted.

Telecommuting, besides, provide numerous benefits to the individual workers, which include better social life, improved time management, flexible working hours, less pressure on workers, and homebound employees' ability to also work (Crandall & Gao, 2005; Nosek, Mandviwalla, & Kock, 1999)

One positive impact of telecommuting on individual workers is that they do not commute back and forth to work and hence can cut down on transportation cost (Hunton, 2005). With cutting down on cost, the individual workers are therefore able to have an improved balance between their work and life at home. Improved job satisfaction leads to highly motivated workers when telecommuting is adopted.

Telecommuting, besides providing numerous benefits to the individual workers which includes better social life, improved time management, flexible working hours, less pressure on workers, and homebound employees' ability to also work (Crandall & Gao, 2005; Nosek, Mandviwalla, & Kock, 1999)

One of the benefits of telecommuting as stated in Garg and van der Rijst (2015:37) is the cost-saving element for the company on office rentals as well as utility bills such as water and electricity. The authors suggest that if telecommuting is elected as a means to work, then a traditional office environment will not be needed as all communication will take place via a virtual platform.

Another benefit as listed by Garg and van der Rijst (2015:37) is the time saved through reduced travel obligations and congestion on the roads. The authors further suggest that this will result in employees enjoying reduced stress and transportation costs. The time spent travelling to work could be utilised on executing work activities. On a larger scale, this would contribute towards a reduction in air pollution, traffic congestion and would also result in employees spending less money on transportation costs.

Another benefit, as stated by Garg and van der Rijst (2015:38), is that telecommuting results in an increased level of productivity as well as improved job satisfaction and higher levels of morale. The authors further suggest that employees that telecommute have the benefit of flexible working hours as well an increase in time spent with their family. The study by Garg and van der Rijst (2015:38) also resulted in fewer sick days being taken and an ultimate increase in overall productivity.

The literature indicates several benefits of telecommuting and Gajendran, Harrison and Delaney-Klinger (2015:3) state that telecommuting can influence key employee outcomes and enhances the employee's experience in the company.

The literature is also specific about telecommuting being a choice and employees having the ability to choose how they prefer to work, but this is not the situation at present with the advent of COVID 19. Telecommuting is a result of the government-imposed regulations, and while some companies have implemented a one-third workforce to return there is a multitude of companies which have remained one hundred per cent virtual.

In considering the array of benefits that telecommuting presents, it is not a suitable working environment for every employee.

While some employees might excel via telecommuting, others may prefer a more traditional working environment where Managers are accessible in-person to handle queries and concerns.

Challenges of Telecommuting

A major challenge, as highlighted by Lewis (2020:4), relates to data privacy and security needs of employees while telecommuting.

One of the downsides of telecommuting, according to Garg and van der Rijst (2015:39) is that employees might tend to lose their identity within the structure of the company. The authors reiterate that the notion of having an identity within the workplace was easier to achieve in a traditional office environment as compared to a virtual space.

Another identified challenge as listed by Baard and Thomas (2012:5) is that employees usually have a sense of belonging and pride as being members if a larger organisation and this can be difficult to maintain in a digital environment.

Garg and van der Rijst (2015:40) highlight that when employees move into an exclusive telecommuting environment, there would be reduced face-to-face communication with a manager and probably less feedback. The authors state that this has the potential to negatively impact on the relationship between the employee and direct supervisors due to continued absences of direct personal contact and interactions.

Further to the above, Garg and van der Rijst (2015:40) posit that working from home creates the additional challenge of employees being interrupted by disturbances at home from kids and everyday activities which might make it difficult to find a balance between the work and home surroundings.

Employee relationships within a work environment can create for a positive and motivating environment, and Garg and van der Rijst (2015:40) argue that this relationship will change when employees telecommute.

The authors suggest that this directly impacts on the employee's ability to build and maintain relationships within the organisation. The atmosphere that is generated when employees work together cannot be replicated with the same warmth and social niceties when using communication tools such as teleconferences and email.

One of the major hurdles, as reiterated in Baard and Thomas (2012:5), is the constant technological advancements relating to faster transfer speeds and mobile connectivity as well as the barrage of online communication tools.

This presents a challenge as it places an additional burden on the employer to ensure that employees have access to the latest technology and connections to ensure an easier and more efficient level of communication.

Operational Risks

Telecommuting presents an exceptional challenge with regards to the vast range of operational risks that it poses. These operational risks can have a detrimental effect on company processes and have the potential to damage the reputation of the company.

COVID-19 creates a new twist for telecommuting employees as the offices are not open, the usual physical work processes have been amended, and the technical infrastructure setup is not available. In addition, employees cannot conduct physical visits to clients, and this creates another impediment in terms of achieving set performance outcomes as all these engagements are expected to occur in a virtual arena.

In the above instances, the employer has a responsibility to ensure that there is proper mitigation of operational risk factors. Operational risks, according to Weeserik and Spruit (2018:2-3) refer to the potential threats resulting from human actions, internal processes and system events which, the authors posit, are the root cause of several large scale financial failures that have afflicted employers.

Types of Operational Risks

Studies highlighted in Weeserik and Spruit (2018:2-3) indicate that operational risks are not a new phenomenon and include a broad range of activities such as human error, fraud, process failures, system errors, cyber threats and external hazards.

The authors submit that the inappropriate management of operational risks can hamper the performance of employees and result in a significant loss. Due to the globalisation of almost every sector within which work is done, operational risks now pose an even bigger threat.

The primary aim of telecommuting is to allow employees to work from anywhere they want to, such as working from public areas but with the onset of COVID-19, telecommuting now refers to working from a virtual home environment. Ngambeket (2017:2) submits that working from a virtual home office causes serious threats to the integrity of data and risks associated with cloud technology.

Ngambeket (2017:2) also highlights that the following are considerations of operational risk when employees telecommute:-

- Loss or damage to assets when in possession of the employee at homes such as laptops, cell phones and tablets.
- Loss or damage to customers data or critical information.
- Cloud technologies and the risks associated with the internet such as viruses, worms and fraud. This also includes risks related to confidentiality and access to programs and data.
- Personal security of the employee and the assets in possession.

Ngambeket (2017:3 - 4) highlights the above-mentioned potential operational risks that employees who are working from home, can encounter.

The employee has to exercise a degree of control and confidentiality when accessing data and systems, and the employer has a reciprocal duty to ensure that the correct measures are in place to mitigate such operational risk factors.

Operational Risks While Telecommuting

Information Systems (IS) form an integral part of daily employee worklifes either by how we communicate through the internet, the banking services we use as well as the software systems available within our working environment. These systems and software play an important role when employees telecommute and are a vital component in ensuring the successful execution of their duties.

Susanto, Almunawar and Tuan (2012:67) indicate that organisational communication channels which use different networks such as an intranet, internet as well as extranet are exposed to the network being infiltrated by hackers.

Further to the above, Degirmenci, Shim and Breitner (2020:2) identify with the flexibility that is provided by telecommuting however they highlight another huge operational risk referred to as Bring Your Own Device (BYOD).

The authors suggest that BYOD allows employees to use their own devices, such as laptops and tablets, to execute their responsibilities. The operational threat that this creates as stated in Degirmenci, Shim and Breitner (2020:2) is that employees will use their software and mobile applications and without the correct anti-virus software this can create major security risks relating to privacy intrusions.

Employee personal devices could contain sensitive corporate information which could be compromised by malware intrusions leading to disastrous effects. If there is no proper management of information systems and devices, loopholes are created for potential cyber threats which could significantly damage a company's reputation and financial position.

While telecommuting provides employees with the flexibility to work from a home space, Jenkins (2020:2) states that this has increased the levels of threats that the employee is exposed to in the form of information threats.

The author highlights that an employee's computer cannot be safeguarded by the company at all times as while surfing the

web or even opening email attachments, certain malicious applications and software might be downloaded.
Jenkins (2020:2) proceeds to state that the security standard at home might not match the corporate office standard and even the anti-virus or software applications on the computer might not be sufficient to deter cyber threats.

Laudon and Laudon (2018:326) refers to malicious software programs such as malware, which includes many threats such as computer viruses, worms and Trojan horses. A computer virus as defined by Laudon and Laudon (2018:326) as a rogue software program that attaches itself to another software program without knowledge and permission of the user, and delivers a 'payload', namely a message to amend, erase or destroy specific software on a computer.

According to Zeidanloo, Tabatabaei & Amoli (2015:342), a worm is a malicious software that can distribute from one computer to another by duplicating itself via the network. A Trojan horse is another form of malware unlike a virus as it does replicate itself, it appears innocent to a user but is a way for a virus to be introduced to a computer.

Laudon and Laudon (2018:328) refer to ransomware which is a form of malware that tries to extort money from users by taking control of their network and computers and accessing personal information. Spyware is a type of malware installs themselves surreptitiously on a computer with the aim of monitoring surfing activity.

In addition to the threat that is posed by malware, Cybercrime has become a concern for businesses and governments based on the ill intention of the Hackers. Businesses are at constant threat of Hackers acquiring access to their systems, banking information, employee information as well as all stored data.

This makes businesses susceptible to intrusion, which can result in funds being stolen, the identity of employees duplicated and even trade secrets being acquired and sold to competitors which is a form of corporate espionage. These threats are heightened when employees telecommute as their computers contain systems and confidential client data, which can be accessed surreptitiously by Hackers.

The threats mentioned above are from external sources; however, employees of a company pose an internal threat to the security of the business. Persons working within a company pose the most prominent security-related threats as they have access to company information and systems and can gain information without any suspicion being attached to them (Fan, Lwakatare & Rong, 2017:1-2).

The opportunity for employees to manipulate systems and inappropriately use sensitive information is amplified when employees telecommute.

Social engineering, according to Abass (2018:258), is the ability to manipulate a device or computer to gain access to certain information or databases. The author highlights that Social engineering is the most successful method of intrusion as compared to others. Social engineering can cripple a business or organisation based on the level of access that employees have to company information.

As working environments are striving for digitisation and automation of their business environments, the concept of flexibility and working remotely from the office becomes relevant.

The concept of Bring Your Own Device (BYOD) according to Pillay, Nham and Tan (2013:1-2) is an effective strategy that allows business partners and employees to use their personal devices such as cell phones, laptops and tablets to use business applications and access data from anywhere.

Telecommuting however creates several vulnerabilities for the business network that the user is accessing. If that personal device was infected with a virus or Trojan Horse, there is a possibility that it could spread onto the network and disrupt the business network. In addition to this, if users are connected to open WIFI networks, there is a possibility of Hackers accessing the personal device and obtaining business information.

Pereira and Santos (2014:2-4) highlight that one of the greatest threats is identity theft which includes the loss of data by organisations that are responsible for safekeeping such data. Due to the increase in crimes of this nature, there has been the development of stringent national and international data protection laws which mandate organisations to protect the personal information of people. (Pereira and Santos, 2014:2-4)

The Canadian Centre for Cyber Security (CCCS) (2020) indicates that when employees work remotely, they would require access to all the internal systems and information that they would normally use when working an office. In addition to this, telecommuting presents a new set of vulnerabilities, and employers have to try and initiate certain precautions to prevent external actors from taking advantage of these vulnerabilities.

Jenkins (2020:2) states that a major risk attached to telecommuting is the physical risk of the computer being stolen. The author posits that in a traditional office setting, there are many layers of access and controlled access to the building as opposed to a home office where there are not as strict measures of access and control.

In addition to this, the CCCS (2020) asserts that if people do not exercise proper control of their devices, there is a threat of people stealing them, whether in a public or private setting.

With increasing reliance on technology to stimulate competitive advantage, the issue of information security poses the most significant threat and challenge to the success of a business while employees telecommute. Even though the systems create an efficient and effective mechanism for the workforce, they also cause a plethora of threats in the form of security issues.

The employer has a responsibility to ensure that there are proper systems and policies in place when employees telecommute. There is a reciprocal duty for the employer to maintain security levels of employee's devices and for the employee to behave responsibly and with the best interest of the company in mind. There is a multitude of measures that the employer can utilise to mitigate the threats explained.

The operational risk mitigation factors, according to Ngambeket (2017:5-6), are vast and are dependent on the company and the specific risks that they are exposed to. The authors suggest measures such as having proper security policies in place and having training and awareness programs for employees.

These risk mitigation factors might not be applicable with the advent of COVID-19 and employers must be creative and inventive when implementing processes to ensure that these factors are catered for. The literature has a comprehensive list of operational risk factors that are heightened when employees telecommute.

There are many ways in which a company can mitigate risks that are associated with telecommuting and information system threats. According to Jenkins (2020:6), a company can have a very detailed security policy which governs telecommuting. The author states that this should contain all aspects related to authorisation, equipment used, software utilisation and even network services that the employee should use.

The policy would serve as the base document, which dictates how work activities should be administered. During the COVID 19 period, many companies moved to an exclusive telecommuting environment, and if they did not have a security policy in place which included telecommuting, then a company would need to develop such policy.

Having a security policy is the initial step in mitigating operational risks while telecommuting; however, the policy would not be beneficial if employees are not made aware of the content. Author Jenkins (2020:7) states that user education is an essential element in ensuring risk mitigation. The author further states that employees need to be taught about security risks and how to prevent them from occurring.

The physical device needs to be protected from potential theft or prying eyes, as suggested by Jenkins (2020:7) as well as ensuring that the appropriate anti-virus software is made available to the employee. The author reiterates that the anti-virus software also needs to be regularly updated and configured to automatically scan all files, including emails.

Further to the anti-virus software Jenkins (2020:7) also states that data needs to be encrypted and protected this way and that the data also needs to be backed up. The author recommends that corporate data be stored on a separate corporate network and not on a computer. If data is stored on a network, it would also allow the employer an opportunity to determine who is accessing information at different times.

In addition to the above risk mitigation measures, the Canadian Centre for Cyber Security (2020) also recommends that employees that are telecommuting only use a business provided device and not a personal one.

The use of personal devices to conduct work activities needs to be restricted as this allows for a barrage of additional security risks. Further to this, the CCCS (2020) indicates that employees need to ensure that they protect the information, including their passwords and that they have access only to information that they need to perform their work responsibilities.

These risk mitigation measures might not have been implemented by companies as they were hoisted into a telecommuting environment due to COVID 19 restrictions. Companies who have not provided for an exclusive telecommuting environment previously would need to assess the security situation and consider following these protocols to minimise risks that might affect employees.

Research Methodology

This study was qualitative utilizing a phenomenological research approach. A phenomenology approach allows for a phenomenon to be explored from the perspective of those who have experienced it. (Neubauer, Witkop and Varpio, 2019:91)

The primary purpose as highlighted by Neubauer, Witkop and Varpio (2019:91)is to describe what was experienced and how this was experienced. The phenomenological approach for this study examined how each elected employee at the company has experienced telecommuting and the individual impact on them achieving their expected performance standards.

A varied representation of employee Respondents from junior, middle and executive functions in the various business units of the organization was sampled based on gender, race, levels of seniority and occupational levels.

The following parameters were set to establish the target population:

- Men and Women
- Between the ages of 24 and 55
- Working for the company in Midrand
- No experience in telecommuting
- Exclusively telecommuting during COVID-19 restrictions.

In addition to the above parameters, the following categories of occupational levels have been determined as follows:

- Technical
- Non-Technical
- Middle and Senior Management
- HR and administrative support

Purposeful random sampling was used to select Respondents.

Data Collection

A standardised, open-ended interview was used to collect data using an interview questionnaire as a guide for the process.

Age Distribution

Age	Population percentage
20-29	37..5%
30-39	25%
40-49	37.5%
Total	100%

Findings From Research

The main findings from the research are tabulated below.

Findings of the Study	Explanation
Effectiveness of telecommuting	Respondents highlighted that telecommuting enabled them to be more effective at executing their work responsibilities whilst telecommuting as opposed to when they work from the office.
Increased Productivity	There was a considerable increase in productivity levels, as highlighted by Respondents. The contributing factors of increased labour productivity levels are based on the heightened focus, greater efficiencies, lower time wastages spent travelling and more time spent working whilst telecommuting.
Enhanced workplace performance	Respondents emphasised that they can work more effectively from home and that their overall performance was enhanced based on their workplace production.
Client Demands	Respondents have indicated that client expectations have increased and the expectations attitude from clients is that Respondents are available at all hours of the day for work issues. The notion of structured working hours has become blurred, and Respondents are now expected to be available for client engagement well beyond the conventional working hours.
Access to Client Database	Respondents do not all have access to the client database, and access is restricted according to the line functional duty of Respondents.
Usage of Cloud Accounts	Respondents indicate that they do not necessarily have documents loaded on their laptops or keep hard copies but that they access these documents via a Google Cloud account.
Increased Company Communication	Respondents indicate that they have received constant communication from the company in terms of company policies and procedures. This relates to their safety and security policies as well as their operational manuals.
Access and Connection	Respondents indicate that they prefer to work from their private devices even though they have been issued with company-work tools (laptops machines).
Connectivity Strain	Respondents indicate that some of them are affected by connectivity issues, and this places a strain on their working parameters. Respondents are subsequently forced to spend more money on expenditure for connectivity and online meetings since not all Respondents were provided with company 3G cards.
Safety and Security Policy	Some Respondents highlighted that they are not sure or not aware if the company has a safety and security policy. These Respondents were unsure about the existence of such policies.
Adjustment of Working Hours	Respondents have indicated that they work long, and irregular hours and they line between the conventional working hours is blurred.
Excessive Meetings	Respondents highlighted that there is an array of meetings that they attend

	daily, and this is either with clients or colleagues.
Lack of Human Interaction	Respondents indicated that whilst they can perform their duties whilst telecommuting; however, they miss the ability to interact with clients and colleagues in person.

While the literature supports the notion that telecommuting employees have more time available to spend with family, this study reports the opposite. The study found that employees telecommuting under COVID lockdown regulations have little to no time to partake in traditional home activities and have little quality family time.

The Respondents work until the late hours of the night, and the working hours are placing a strain on the home environment. This has the potential to have a negative long-term effect on the Respondents and can hamper the efficacy of telecommuting.

Some of the challenges as revealed by the literature review related to the lack of face to face interaction as well as the disturbances at home which could make it strenuous on Respondents striking a balance between their home and work responsibilities.

These two notions were also highlighted by two Respondents of this study who emphasised that they miss the office interaction with colleagues, and they feel that they would prefer working in an office environment based on this factor.

A common theme shared by Respondents is that finding a balance between work and their home lives has been one of the major barriers they encountered whilst telecommuting.

Respondents indicated that they struggled whilst telecommuting in the beginning, especially due to COVID19 regulations and having to homeschool children and manage other commitments at home.

The literature highlighted the variety of operational risks that exist such as human error, fraud, process failures, system errors, cyber threats and external hazards.

This study found that the major operational risks identified could come from Cloud technology, using personal devices, no mandate anti-virus software and cyber threats that could flow from this, including privacy intrusions.

Many Respondents indicated that they use personal devices instead of the company issued one and that anti-virus software is not mandated by the organisation.

In an attempt to mitigate the operational risks, the literature denotes that merely having a security policy is not sufficient as there needs to be an awareness of the contents of the policy. This study found that some Respondents were not aware that a security policy exists and the Respondents who knew of the existence of the security policy, did not know the actual contents of the policy and what applies to them.

Recommendations of Study

Based on the research problems and the findings of the study, some practical recommendations are hereby put forth to enhance employee performance and reduce operational risks.

The identified areas for improvement are as follows:

- Closer Management of Client relationships:
- Monitoring of Virtual Databases for Information Security:
- Ensuring Higher Staff Awareness of Organisational Policies:
- Instilling Better Time Management by Staff:
- Continued Team Building:
- Acknowledgement and Rewards:
- More Workshop Sessions to Combat Operational Risks

Bibliography

ABASS, I.A.M. 2018, 'Social Engineering Threat and Defense: A Literature Survey', *Journal of Information Security*, vol. 09, no. 04, pp. 257–64.

ALON,T.M, DOEPKE, M. & OLMSTEAD-RUMSEY, J.2020, The impact of COVID-19 on gender equality, Journal of Chemical Information and Modelling.

Allen, T.D., Golden, T.D. & Shockley, K.M.2015,'How effective is telecommuting? Assessing the status of our scientific findings', Psychological Science in the Public Interest, vol.16, no. 2, pp.40-68.

AL TAJIR, G.K. 2018, 'Ethical treatment of participants in public health research', Journal of Public Health and Emergency, vol.2,pp. 2-2.

ANGELES,S.2019. Remote Workers Success Starts With It Support [Online]. Available from buisnessnewsdaily.com/ [Accessed:17 June 2020].

ASIAMAH,N., MENSAH, H.K. & OTENG-ABAYIE, E.F.2017, ,General, target and accessible population: Demystifying the concepts for effective sampling', Qualitative Report, vol.22, no. 6, pp. 1607-21.

BAARD,N.& THOMAS, A.2010, 'Teleworking in South Africa: Employee benefits and challenges', S.A. Journal of Human Resource Management, vol.8, no.1.

BELZUNEGUI-ERASO, A. & ERRO-GARCÉS, A. 2020, 'Teleworking in the Context of the Covid-19 Crisis', *Sustainability*, vol. 12, no. 9, p. 3662.

BHAT, S.K., PENDE, N.& AHUJA, V.2017, ,Virtual Team Effectiveness: An Empirical Study Using SEM', Procedia Computer Science, vol.122, pp.33-41.

BOROWSKA-BESZTA, B .2017, 'Decoding of Bias in Qualitative Research in Disability Cultures: A Review and Methodological Analysis', International Journal of Psycho Educational Sciences, vol. 6, no.3,pp.55-68.

BORU,T. 2018, 'Chapter five research and design methodology 5.1. Introduction Determinants of Bank Selection choices and customer Loyalty the case of Ethiopian Banking Sector View project, Research Design and Methodology.

CANADIAN CENTRE FOR CYBER SECURITY.2020. [Online]. Available from: http ://cyber.gc.ca/ [Accessed 11/06/2020].

CONCEICAO, S.C.O., SAMUEL, A.& YELICJ BINIECKI, S.M. 2017, ' Using concept mapping as a tool for conducting research: An analysis of three approaches', Cogent Social Sciences, vol.3, no.1.

DANIEL,E.2016, 'The Usefulness of Qualitative and Quantitative Approaches and Methods in Researching Problem-Solving Ability in Science Education Curriculum', Journal of Education and Practice, col.7,no.15,pp.91-100.

DEGRIMENCI, K., SHIM,J.P.& BRIETNER,M.H.2020, Future of flexible work in the digital age: Bring you own device challenges of privacy protection, 40th International Conference on Information Systems, ICIS 2019.

DJANDA,H., MADDELEINE, L& KRISTINA, R.2018,'Managing a stressful work environment through improved teamwork-A Qualitative Content Analysis of nurses working environment within emergency care', International Archives of Nursing and Health Care,vol.4,no.4,pp.1-9.

ELO, S., KAARIAINEN, M. & KANSTE, O. 2014, ,Qualitative Content Analysis', SAGE Open, vol.4,no.1,p215.

ETIKAN, I.2017, 'Sampling and Sampling Methods', Biometrics and Biostatistics International Journal, vol.5, no.6, pp.215-7.

FAN,W., LWAKATARE,K.& RONG, R.2017, 'Social Engineering: I-E based model of Human Weaknesses for Attack and Defense Investigations ', International Journal of Computer Network and Information Security, vol.9,no.1,pp.1-11.

GAJENDRAN, R.S., HARRISON, D.A.& DELANEY-KLINGER,K. 2015, 'Are Telecommuters Remotely Good citizens/ Unpacking telecommuting's effects on performance via Deals and job resources', Personnel Psychology,vol.68,no.2,pp.353-93.

GARG,A.K.& VAN DER RIJST, J. 2015, ,The benefits and pitfalls of employees working from home: Study of a private company in South Africa', Corporate Board: Role, Duties and Composition, vol.11,no. 2,pp.36-49.

GUREL, C. & TAT, M. 2017, 'SWOT Analysis: A Theoretical Review', Journal of International Social Research, vol.10,no.994-1006,pp.45-56.

HAMMARBERG, K., KIRKMAN, M.& DE LACEY, S. 2016, , Qualitative Research methods: When to use them and how to judge them', Human Reproduction, vol.31,no. 3, pp.498-501.

ISMAIL, N., KINCHIN, G. & EDWARDS, J-A. 2017, ' Pilot Study, Does It Really Matter? Learning Lessons from Conducting a Piot Study for a Qualitative PhD Thesis', International Journal of Social Science Research, vol. 6, no. 1, p.1.

JACKSON, L.T.B.& FRANSMAN, E.I. 2018, 'Flexi work, financial well-being, work-life balance and their effects on subjective experiences of productivity and job satisfaction of females in an institution of higher learning', South African Journal of Economic and Management Sciences, vol.21, no.1, pp.1-13.

JENKINS, G. 2020, Information Security Reading Room Designing a DMZ-Mitigating teleworking risks.

KRUGEL, L. & VILJOEN, C. 2020, Impact of trade disrupting COVID-19 on South African business, February.

LAUDON, K. AND LAUDON, J. 2018. Management Information Systems: Managing the Digital Firm. 15th ed. England: Pearson Education, pp.42-44.

LEUNG L. VALIDITY, 2015. Reliability and Generalisation in qualitative research. J Family Med Prime Care 2015: p.p,324-7.

LEWIS, J. 2020, 'Work-from -home checklist during the coronavirus pandemic', The National Law Review, pp.1-4.

LINDÉN, A. & OLJEMARK, S. 2018, Degree project in the field of technology ManagingTelework.

LONG, H. 2014, 'An empirical review of Research Methodologies and Methods in creativity studies', Creativity Research Journal, vol.26, no.4,pp.427-38.

MALMQVIST, J., HELLBERG, K. & MOLLAS, G. 2019, "Conducting the Pilot Study: A Neglected Part of the Research Process? Methodological Findings Supporting the Importance of Piloting in Qualitative Research Studies', International Journal of Qualitative Methods, vol.18,pp.1-11.

MITCHELL, A. 2018, 'A review of mixed methods, pragmatism and abduction techniques', Electronic Journal of Business Research Methods, vol.16, no.3,pp.103- 116.

MOHAJAN, H. & MOHAJAN, H.K. 2018, 'Munich Personal RePEc Archive Qualitative Research Methodology in Social Sciences and Related Subjects Qualitative Research Methodology in Social Sciences and Related Subjects', *Journal of Economic Development, Environment and People*, vol. 7, no. 85654, p. 1.

MUKHERJI, P. & ALBON, D. 2014, 'Research Methods in early Childhood', *SAGE Open*, Los Angeles, p. 97.

NAMUGENYI, C., NIMMAGADDA, S.L. & REINERS, T. 2019, 'Design of a SWOT analysis model and its evaluation in diverse digital business ecosystem contexts',*Procedia Computer Science*, vol. 159, pp. 1145–54.

NATIONAL ACADEMIES OF SCIENCES, T. 2017, *Fostering Integrity in Research A Consensus Study Report of*.

NEUBAUER, B.E., WITKOP, C.T. & VARPIO, L. 2019, 'How phenomenology can help us learn from the experiences of others', *Perspectives on Medical Education*, vol. 8, no. 2, pp. 90–7.

NGAMBEKET, G. 2017. Mobile Workforce Security Considerations and Privacy, *ISACA Journal*, vol. 4, pp. 18–23.

NOWELL, L.S., NORRIS, J.M. & WHITE, D.E. 2017. Thematic Analysis: Striving to Meet the Trustworthiness Criteria', *International Journal of Qualitative Methods*, vol. 16, no. 1, pp. 1–13.

ONYEMAECHI, U., CHINYERE, U.P. & EMMANUEL, U. 2018. Impact of Telecommuting on Employees' Performance, *Journal of Economics and Management Sciences*, vol. 1, no. December, p. p54.

PARADIS, E., O'BRIEN, B. & NIMMON, L. 2016. Design: Selection of Data Collection Methods, *Journal of graduate medical education*, vol. 8, no. 2, pp. 263–4.

PILLAY, A., NHAM, E., TAN, G. & DIAKI, H. 2013. Does BYOD increase risks or drive benefits?, *Dtl.Unimelb.Edu.Au*, no. 2013, pp. 1–8.

PEREIRA, T. & SANTOS, H. 2014. Challenges in Information Security Protection, *Proceedings of the 13Th European Conference on Cyber Warfare and Security (Eccws-2014)*, no. July, pp. 160–6.

RAHMAN, M.S. 2016. The Advantages and Disadvantages of Using Qualitative and Quantitative Approaches and Methods in Language "Testing and Assessment" Research: A Literature Review', *Journal of Education and Learning*, vol. 6, no. 1, p. 102.

RICHARD, L. 2012. Telecommuting : Implementation for Success, *International Journal of Business and Social Science*, vol. 3, no. 15, pp. 20–30.

RIDDER, H.G. 2017. The theory contribution of case study research designs', *Business Research*, vol. 10, no. 2, pp. 281–305.

REBECCA, B. 2016, *Types of Research Designs*, South Carolina.

SALVADOR, J.T. 2016. Exploring Quantitative and Qualitative Methodologies: A Guide to Novice Nursing Researchers, *European Scientific Journal, ESJ*, vol. 12, no. 18, p. 107.

SCHALL, M.A. 2019. The Relationship Between Remote Work and Job Satisfaction :The Mediating Roles of Perceived Autonomy , Work-Family Conflict , and Telecommuting Intensity, San Jose State University.

SEKYERE, D.E., BOHLER-MULLER, P.N. & HONGORO, P.C. 2020, *Africa program occasional paper*.

SUSANTO, H., ALMUNAWAR, M.N. & TUAN, Y.C. 2012, Information Security Challenge and Breaches : Novelty Approach on Measuring ISO 27001 Readiness Level, *International Journal of Engineering and Technology*, vol. 2, no. 1, pp. 67–75.

TAHERDOOST, H. 2016. Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research, *International Journal of Academic Research in Management (IJARM)*, vol. 5, no. January 2016, pp. 18–27.

UGARGOL, J. P. H. 2018. The Relationship of Workplace Flexibility to Employee Engagement among Information Technology Employees in India. South Asian Journal of Human Resources Management.

WANG, Y., LI, G. & LI, J. 2018. Comprehensive identification of operational risk factors based on textual risk disclosures', *Procedia Computer Science*, vol. 139, pp. 136–43.

WEESERIK, B.P. & SPRUIT, M. 2018. Improving Operational Risk Management using Business Performance Management technologies', *Sustainability (Switzerland)*, vol. 10, no. 3.

ZEIDANLOO, H.R., TABATABAEI, F. & AMOLI, P.V. 2015. 'All About Malwares (Malicious Codes).', *Security and Management*, no. i, pp. 342–8.