# Understanding the role of cybersecurity culture in the gig economy: The case of platform-based food delivery workers in Gauteng


A Dissertation presented to the

Department of Information Systems

University of Cape Town

by

Mlungisi Radebe

*RDBMLU003*

Supervisor
Pitso Tsibolane

In partial fulfilment of the requirements for Master of Commerce: Information Systems

**Declaration**

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.
2. I have used the APA convention for citation and referencing. Each contribution to, and quotation in, this paper entitled *Understanding the role of cybersecurity culture in the gig economy: The case of platform-based food delivery workers in Gauteng* from the work(s) of other people has been attributed and has been cited and referenced.
3. This paper is my own work, part of which formed earlier submissions to the University of Cape Town.
4. I have not allowed, and will not allow anyone, to copy my work with the intention of passing it off as his or her own work.
5. I acknowledge that copying someone else's assignment, essay or paper, or part of it, is wrong, and declare that this is my own work.

Signed by candidate

---

Mlungisi Radebe

RDBMLU003

Date: 16 February 2025

## Acknowledgements

*In all sincerity, I want to express my gratitude to my partner, Sinemihlali, for her unwavering support and patience. To my son, Bakang, for his boundless happiness and motivation, and to my supervisor, Mr Pitso Tsibolane, for providing me with essential direction and encouragement. Knowing that they have faith in me has been helpful along this road, and I am incredibly grateful to them for their love, knowledge, and understanding.*

## Abstract

The growth of gig economy platforms has coincided with increased cybersecurity threats and attacks. As gig platforms have evolved, so too have cybercriminals, with attacks such as malware, phishing, and social engineering becoming increasingly sophisticated and human-centric. However, cybersecurity defence mechanisms are still centred around traditional technical controls. In response to this growing threat landscape, researchers argue that organisations should implement other mechanisms to counter the threat. Embedding a cybersecurity culture in organisations has gained prominence in recent studies. However, studies on the cybersecurity culture in the gig economy, focusing on food delivery workers, are needed, as there is currently limited literature on this phenomenon. This research report explored the nature of cybersecurity culture in the context of platform-based food delivery workers in Gauteng, South Africa. The main research question explored the following: How does the cybersecurity culture influence the cybersecurity behaviours of food delivery gig workers?

The Cybersecurity Culture Model (CCM) was used as a sensitizing theoretical device to develop the initial interview guides, observation protocols, and the preliminary coding schemes. A qualitative research strategy was adopted using semi-structured interviews as the primary data source; furthermore, a qualitative research survey and publicly available documents and observations of the context were provided as secondary data sources. Fifteen (*N=15*) semi-structured interviews were performed with food delivery workers. Secondary data was acquired via online searches (*N=11*), web articles on the gig economy, three (*N=3*) online qualitative surveys, and contextual observations by interacting with food delivery workers at their pick-up sites. Data analysis was conducted using established guidelines for inductive data analysis using the NVivo 14 software.

The research revealed significant barriers to implementing cybersecurity culture in the food delivery sector of the local gig economy. Workers receive minimal cybersecurity education and training, with limited management communication about security policies and procedures. Gig work apps present additional challenges, contributing to a virtually non-existent cybersecurity culture among food delivery workers in Gauteng, South Africa. Weak management initiatives, inadequate training, and absent security policies drive non-compliance, further complicated by conflicts between financial incentives, personal safety, and cybersecurity requirements. These findings highlight structural gig economy issues, underscoring the need for enhanced cybersecurity governance, comprehensive training programs, and integrated information security policies. Future research should examine platform providers' responsibilities in cybersecurity culture development and methods to align safety priorities with cybersecurity compliance.

Keywords: *Cybersecurity Culture, Training and Awareness, Top Management Support, Information Security Policies and Procedures, Personal Safety, Cybersecurity Culture Model*

Table of Contents

## List of Tables



## List of Figures

## List of Acronyms

Information and Communication Technology - ICT

Bring Your Own Device - BYOD

Beliefs, Values, and Attitudes - BVAs

Security, Education, Awareness, and Training - SETA

Cybersecurity Culture Model - CCM

Information Security Policy - ISP

# 1 Introduction

## 1.1 Background of Study

Over the last decade, cybersecurity issues have remained a concern, with exacerbated and pervasive cyberattacks regularly occurring (Chakkaravarthy et al., 2019). Most of these attacks have identified the humanistic element as being the weakest link in the chain and the primary cause of the attacks. Major cyberattacks with human elements include phishing, viruses and malware, ransomware, and trojans (Alshaikh, 2020; Georgiadou, Mouzakitis, et al., 2022a). Furthermore, cybersecurity has gained attention in human-computer interaction research as more incidents are reported (Breen et al., 2022).

Studies in cybersecurity have predominantly been technically focused, and more scholars argue that cybersecurity should not only be seen as a technical issue; organisations must also depend on employee behaviour for protection (Alshaikh, 2020; Da Veiga et al., 2020). However, organisations still face numerous challenges in ensuring that information technology systems are adequately protected against cybercrime (Masombuka et al., 2018; Subashini et al., 2020). It has been argued that organisations with an embedded cybersecurity culture reduce related cybersecurity risk, leading to fewer severe cyber incidents. Furthermore, organisations reported improved levels of employee cybersecurity awareness (Da Veiga et al., 2020; Huang & Pearlson, 2019).

One area that has generally yet to be explored is the intersection of the gig economy and cybersecurity, which remains a grey area in the literature. The accelerated adoption of Information and Communication Technology (ICT) over the last decade has heightened the prevalence of the gig economy (Anwar & Graham, 2021; Malik et al., 2021). However, this rapid expansion may come at the cost of increased cybersecurity issues for the company and individuals. It has been noted that gig economy workers still have access to company data after leaving employment. Additionally, these employees must be made aware of company security policies and the importance of cybersecurity (Beyond Identity, 2023; Furnell & Shah, 2020). Furnell and Shah (2020) further argue that cybersecurity policies and practices should be adequately ventilated to gig workers by the hiring company to ensure that gig workers can make informed decisions related to cybersecurity.

## 1.2 Problem Statement

A Gartner report published in 2021 estimated that by 2025, every country would have a labour force of over 35% participating in the gig economy (Gartner, 2021). Furthermore, this sector is estimated to expand to a revenue of $335 billion by 2025 (Ungureanu, 2019). Studies concerning the gig economy, platform-based workers in particular, have been primarily focused on how the gig economy has introduced vulnerabilities and challenges regarding algorithmic management (Veen et al., 2020; Vignola et al., 2023; Wood, 2021b), worker precarity (Anwar & Graham, 2021; Bajwa et al., 2018;

Wang et al., 2022) and gig worker training (Furnell & Shah, 2020). However, gig workers' cybersecurity behaviours remain an area that must be explored.

The body of work concerning cybersecurity culture remains in its infancy, with scholars contending that additional investigation is necessary within this domain. (Alshaikh, 2020; Gcaza & Von Solms, 2017). Furthermore, there exists a lack of consensus among researchers regarding a definitive measurement criterion for cybersecurity culture within organisations. The academic landscape has various conceptual frameworks, yet no universally accepted measurement has emerged (Uchendu et al., 2021). Studies have been critiqued for utilising predominantly quantitative methodologies, such as surveys and questionnaires, which are inadequate for measuring cybersecurity behaviour (Jeong et al., 2019; Uchendu et al., 2021). This investigation employed a qualitative methodology that was appropriate for this inquiry. Close interactions with the participants enabled the researcher to acquire firsthand and real-world experience with them. Finally, there is a lack of understanding regarding the factors that affect the cybersecurity behaviours of gig economy workers in academic research. This research investigated the significantly underexamined subject. Therefore, a study of the cybersecurity culture influence on the cybersecurity behaviours of food delivery workers within the gig economy in Gauteng, South Africa, was proposed.

### 1.3 Research Context

The gig economy in South Africa has primarily been driven by the vast unemployment rate, particularly among the country's youth. According to Statistics South Africa, the unemployment rate as of quarter 1, 2023, was 42.6%, and 62.1% of the overall number were youth aged between 15 and 24 (Statistics South Africa, 2023). Furthermore, uptake in the gig economy has also been driven by the increased use of mobile technology and connectivity infrastructure in South Africa (Van Belle et al., 2023). The study focused on food delivery gig workers in Gauteng, South Africa. Gauteng is considered the economic hub of South Africa and is rapidly increasing (Meyer, 2021). Moreover, Gauteng possesses a greater quantity of food delivery services, and the Gauteng Provincial Government has committed an additional 10,000 motorcycles to boost the sector (TimesLive, 2023).

Consistent with the proposed research topic, South Africa has experienced a notable rise in cybercrime activities over the past decade. The incidence of cybercrime in South Africa rose by 8% from 2021 to 2022, with 56 individuals per 1 million Internet users victimised by cybercrime. (Surfshark, 2022). The concentration of reportable cybercrime activities within a particular region determines the cybercrime density ranking (Herley, 2014). Furthermore, Surfshark (2022) indicates that South Africa is ranked number 5 globally and 1 in Africa regarding cybercrime density, see Figure 1 below.

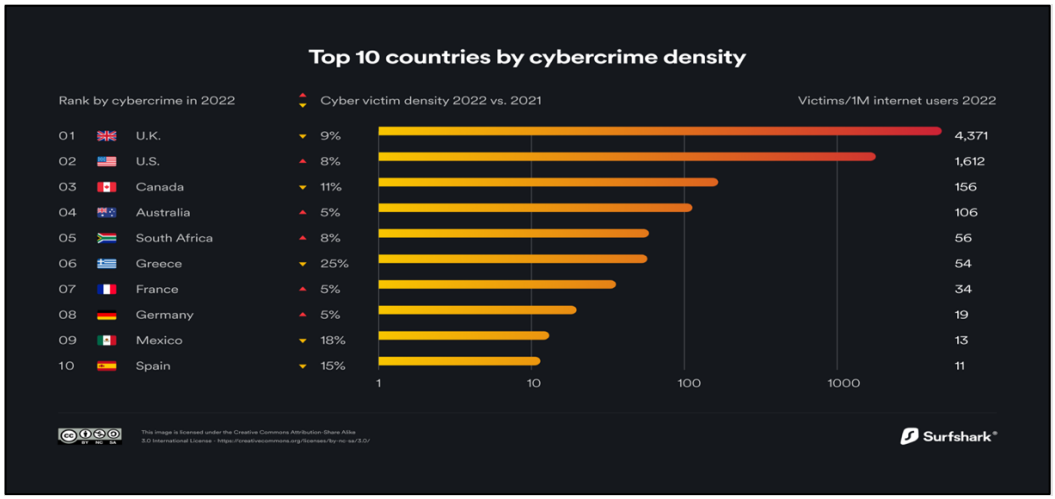



Figure 1. Top 10 Countries by Cybercrime Density (Surfshark, 2022)

During the project, the following research objectives were investigated:

## 1.4 Research Objectives

**A.** To determine how cybersecurity culture influences food delivery gig workers cybersecurity behaviour.

**B.** To describe the cybersecurity cultural factors that influence food delivery gig workers cybersecurity behaviour.

The following questions were answered to address the research problem that has since been faced:

## 1.5 Research Questions

**A. Primary research question**: How does the cybersecurity culture influence the cybersecurity behaviours of food delivery gig workers?

**B. Secondary research question**: What factors influence cybersecurity culture among food delivery gig workers?

## 1.6 Study Significance

This study sought to contribute to the body of work in information systems, specifically to behavioural factors related to cybersecurity among food delivery workers in Gauteng, South Africa. In addition, the study aimed to provide practical suggestions to companies and decision makers on an approach for implementing reliable cybersecurity practices for food delivery workers in Gauteng, South Africa.

# 2 Literature Review

This chapter outlines this study's principles and concepts, including cybersecurity concepts, cyber threats, cybersecurity culture, the benefits of cybersecurity culture, factors that promote cybersecurity culture, and the challenges of cybersecurity culture. Furthermore, this chapter outlines the gig economy, the benefits, and challenges of the food delivery sector. The information included in the literature review was sourced from reputable online academic resources.

## 2.1 Cybersecurity

In a world where technology is advancing at an unprecedented rate, cybersecurity has become a crucial aspect of our daily lives. The term "cybersecurity" originates from combining the prefix "cyber", which is shortened from the original concept of cybernetics (Bay, 2016). Cybernetics was first coined by Norbert Wiener (1948), which refers to the relationship between animals, mechanical systems, and the information loop between them (Wiener, 2019). "Security", the suffix, refers to the protection against threats (Bay, 2016). The words brought together are known as cybersecurity.

Cybersecurity has been defined in multiple ways over the last decade; one definition states that cybersecurity is a sphere of technology focused on deterring threats that originate from many avenues through a combination of technologies (Chaudhary et al., 2020; Li, 2018; Ndlovu & Tsibolane, 2025). However, for this research, the following definition will be adopted, "Cybersecurity is the organisation and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" (Craigen et al., 2014, p. 17). This definition aligns with the holistic concept of organisational cybersecurity culture, which sees cybersecurity as a socio-technical issue and encompasses the legal aspect of cybersecurity.

Cybersecurity issues over the last decade have remained a concern, with exacerbated and pervasive cyberattacks regularly occurring (Chakkaravarthy et al., 2019). As of 2022, it is anticipated that more than 4.7 billion individuals are active Internet users, all vulnerable to cyberattacks (Shillair et al., 2022). Researchers have identified prominent cyberattacks with human elements; these include phishing, viruses and malware, ransomware, and trojans (Alshaikh, 2020; Georgiadou, Mouzakitis, et al., 2022b). Furthermore, Verizon reported that in 2022, 5212 data breaches were reported, with over 80% of the data breaches involving a human element (Verizon, 2022).

The gig economy is increasingly threatened by cyberattacks, as evidenced by Uber's significant data breach in 2016 (Kamais, 2019). This has remained persistent as cyberattacks in the digital economy remain a challenge (Ashrapova & Apsilyam, 2025). These challenges highlight the vulnerable nature of even the most recognised platforms in this area, emphasising the critical necessity for stringent security measures to safeguard sensitive user information. Furthermore, data privacy in the gig economy has attracted the attention of researchers, who argue that it should be an area of concern and that more

research needs to be undertaken (Liang et al., 2022; Tan et al., 2021). In recent years, researchers have argued that cybersecurity should not be seen only as a technical issue; to withstand and protect themselves against pervasive cyberattacks, organisations also need to depend on employee behaviour (Alshaikh, 2020; Da Veiga et al., 2020; Georgiadou, Mouzakitis, et al., 2022a; Huang & Pearlson, 2019; Moletsane & Tsibolane, 2020). Additionally, research suggests that by 2027, more than 50% of large organisations will have adopted a human-centric approach to cybersecurity challenges (Gartner, 2023). Researchers present the concept of organisational cybersecurity culture, which examines cybersecurity via a socio-technical lens (Greitzer et al., 2018; Jeong et al., 2019).

## 2.2 Cyber Hygiene

Cybersecurity risks remain significant, especially within the food delivery sector, where delivery workers bear responsibility for the cyber hygiene of their devices. Cyber hygiene is a relatively new concept adopted from personal hygiene in healthcare literature (Vishwanath et al., 2020). Cyber hygiene has only been described conceptually in literature, with no consensus on what it holistically entails. Vishwanath et al. (2020, p2) describe cyber hygiene as "the cyber security practices that online consumers should engage in to protect the safety and integrity of their personal information on their Internet enabled devices from being compromised in a cyber-attack". Another author describes cyber hygiene as the overall practice and continuous routines followed to ensure the safety and security of online platforms (Ncubukezi et al., 2020). Both definitions of cyber hygiene include the practices and steps users of computers and mobile devices take, to maintain a secure online security presence to deter cyberattacks (Kioskli et al., 2023; Vishwanath et al., 2020). Cyber hygiene can directly influence the organisation's cybersecurity culture; best practices are described in the literature for cyber hygiene to be effective. Figure 2 below summarises some of the best practices identified in the literature to promote healthy cyber hygiene.

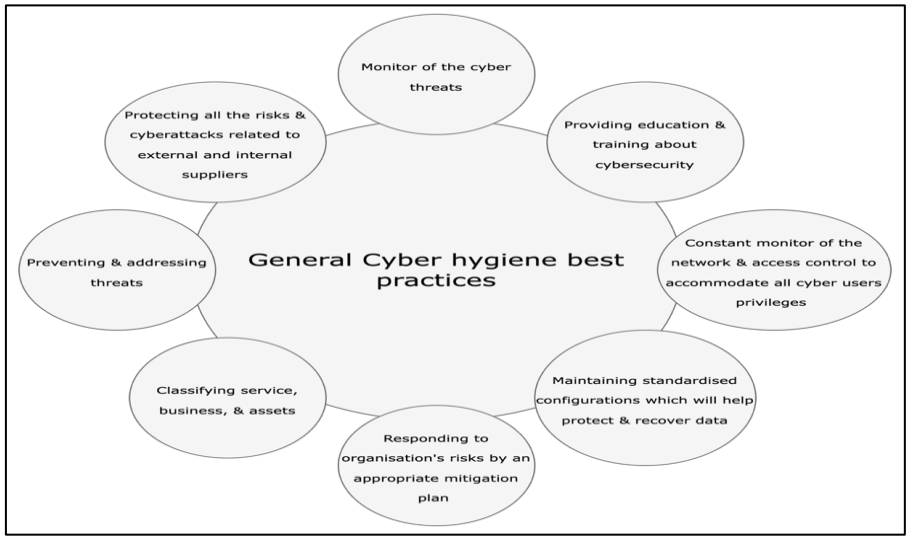



Figure 2 Cyber Hygiene Best Practices (Kioskli et al., 2023)

### 2.2.1 Cybersecurity Risks

The World Economic Forum's Global Cybersecurity Outlook 2024 Insight report highlights that 29% of organisations worldwide have been materially affected by cyber related incidents (World Economic Forum, 2024). This statistic emphasises the pressing need for businesses to invest in robust security measures to safeguard their data and prevent cyber-attacks. The following section will explore some of the prominent cybersecurity risks.

#### 2.2.1.1 Insider Threats

Humans are regarded as the most significant vulnerability in cybersecurity breaches (Kioskli et al., 2023; Rohan et al., 2021). Humans are vulnerable to numerous attacks, including social engineering, targeted malware, and mistakes made by humans (Mazzarolo & Jurcut, 2019). Additionally, insider threats may also be deliberate in committing fraud, intellectual property theft, corporate espionage, and unintentional insider threats (Georgiadou, Mouzakitis, et al., 2022a; Mazzarolo & Jurcut, 2019). All these intentional or unintentional insider threats can directly impact the confidentiality, integrity and availability of information systems if not attended to (Georgiadou, Mouzakitis, et al., 2022a; Mazzarolo & Jurcut, 2019).

However, there are measures that organisations can take to mitigate insider threats. These measures may require a robust combination of access controls, continuous employee monitoring, employee training, stringent background checks, and an organisational cybersecurity culture (Gartner, 2021; Mazzarolo & Jurcut, 2019).

#### 2.2.1.2 Bring Your Own Device

Bring your own device (BYOD) is a policy that allows employees or food delivery workers to use their electronic devices for work purposes (Chen et al., 2021). Food delivery workers can use personal electronic devices, such as smartphones, laptops, and tablets, for both work and personal purposes. This working model benefits the organisation through reduced costs, increased productivity, and greater employee flexibility, which are significant factors in the gig economy (Chen et al., 2021; Ratchford et al., 2022).

However, these electronic devices are inherently susceptible to security risks, and organisations are encouraged to address these risks to mitigate the risk of security breaches (Chen et al., 2021; Ratchford et al., 2022). According to industry reports, the BYOD security market was estimated at US $27.51 billion in 2022 and is projected to reach US $295.75 billion in 2030 (SNS Insider, 2023). Figure 3 highlights the projected growth in revenue for the BYOD security market from 2023 to 2030. Organisations are encouraged to develop policies that clearly define the acceptable use of devices, provide the necessary infrastructure to support the use of personal devices, and provide training and

technical support for the use of devices (Ratchford et al., 2022). However, recent studies have highlighted that organisations still deal with privacy and security issues regarding BYOD (Almarhabi et al., 2023; Ayedh M et al., 2023).

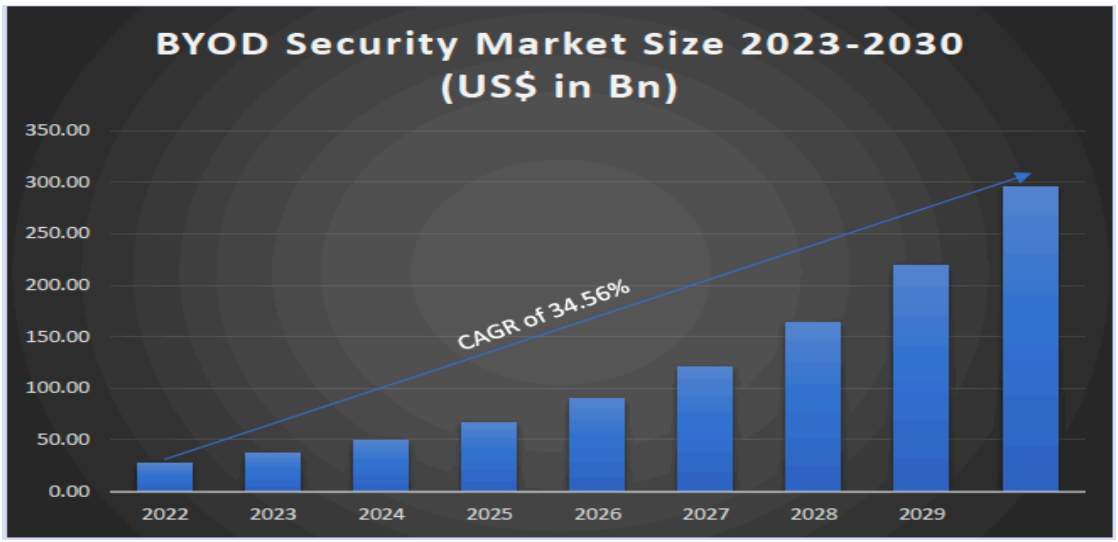



Figure 3 BYOD Security Market Size (SNS Insider, 2023)

#### 2.2.1.3 Cybersecurity Attacks

There are various cybersecurity attacks that are targeted at the weakest element in the cybersecurity chain, these include: malware, phishing, and social engineering.

- **Malware**

Malicious software, or malware for short, is a program that is intentionally designed to cause harm to computer programs and hardware (Chakkaravarthy et al., 2019). Malware can be deployed in various ways, such as ransomware, trojans, worms, rootkits, and viruses. This method can compromise the individual's computers and mobile by leaking sensitive data, tracking movements and altering data (Almarhabi et al., 2023; Dasgupta et al., 2022). Malware is still considered a significant cybersecurity issue, with the 2024 State of Cybersecurity report indicating that Ransomware attacks have increased by an average of 14% yearly since 2021 (Splunk, 2024).

- **Phishing**

Another prevalent cybersecurity risk is called phishing attacks; these are attacks where adversaries disguise themselves as ethical entities to deceive users into divulging sensitive information, such as credit card data, login credentials, and other personal information (Abdillah et al., 2022; Desolda et al., 2021). Phishing has become widespread and sophisticated over the last two decades, creating significant risks for individuals and businesses; the sophisticated attacks include email phishing and spear phishing, which is more targeted and involves tailored emails, smishing; attacks conducted through the use of

short messaging services (SMS), and more recently vishing; an attack where voice calls are used to imitate legitimate individuals or businesses to gain confidential information (Ali & Mohd Zaharon, 2024; Desolda et al., 2021).

- **Social engineering**

Social engineering is another sophisticated cybersecurity attack that exploits humans to gain unauthorised access to resources and information (Ali & Mohd Zaharon, 2024). These attacks can take various forms, such as phishing, pretexting, or baiting, posing significant risks to individuals and organisations.

## 2.3 Organisational Cybersecurity Culture

### 2.3.1 Culture

Groups and communities with a standard belief system remain connected through their shared culture, often called "societal culture" (Schein, 2004). Culture has been cited as far back as biblical times, and the phenomena of culture can be understood in many different ways (Raeff et al., 2020). It is also worth noting that research has also indicated that societal or shared culture can influence behaviours and attitudes (Raeff et al., 2020). Organisational culture is a subset of societal culture, described as the shared values prevalent across a group (Butler & Brown, 2023; Schein, 2004). These shared values can be attributed to the organisation's successes and failures (Sutton & Tompson, 2024). Organisational culture, furthermore, has been noted to have a direct influence on the attitudes and behaviours of employees towards cybersecurity, which directly influences the employee's adherence to security policies and procedures (Karlsson et al., 2022; Solomon & Brown, 2021).

Cybersecurity culture is a subset of organisational culture and is directly influenced by the organisation's strategic direction. Furthermore, cybersecurity culture is noted as an integral component of organisational culture (Amankwa et al., 2022; De Silva, 2023; Huang & Pearlson, 2019). Numerous studies have been undertaken throughout the years that establish a direct correlation between organisational culture and security measures inside organisations, as shown in Table 1 below:

| **Organisational Culture and Security Culture** | | |
|---|---|---|
| **No** | **Author** | **Discussion** |
| **1** | Solomon and Brown (2021) | The research paper investigates the influence of organisational and information security cultures on employees' compliance with information security policies. Findings note that control-oriented |

| Organisational Culture and Security Culture | | |
|---|---|---|
| | | cultures enhance compliance, with goal-oriented practices having a more substantial impact than rule setting. This paper highlights the need for well embedded security communication within organisational cultures. |
| **2** | De Silva (2023) | This paper discusses how a robust organisational culture promotes cybersecurity by aligning employee behaviours with security practices through common factors such as leadership support, policies, and awareness programs. It further highlights that the alignment enhances resilience against cyber threats by bolstering shared responsibility and vigilance. |
| **3** | Amankwa et al. (2022) | This paper underscores the pivotal role of leadership in fostering a supportive organisational culture. Effective leadership, accountability, and user involvement shape a culture where compliance with security policies becomes a shared norm. The paper further highlights that aligning organisational and cybersecurity cultures strengthens the overall commitment to compliance with information security. |
| **4** | Da Veiga et al. (2020) | This paper suggests that aligning organisational and cybersecurity culture not only supports a robust cybersecurity culture but also significantly reduces human-related cybersecurity incidents. The alignment bolsters data protection practices by fostering trust, compliance, and employee engagement in cybersecurity practices and opens the door to a more secure environment. |

Table 1 Organisational Culture and Security Culture

### 2.3.2 Cybersecurity Culture and Information Security Culture

Cybersecurity culture is often used interchangeably with information security culture (Mwim & Mtsweni, 2022; Uchendu et al., 2021). However, researchers have argued that the two concepts should not be confused, as information security culture is focused in the confines of an organisation and cybersecurity culture extends beyond the organisation (Mwim & Mtsweni, 2022; Reid & Van Niekerk, 2014). This extension may include factors that are beyond the organisation's control, factors like

national or regional culture, employee personality traits, and the activities of other organisations that have a direct influence on the cybersecurity culture (Marotta & Pearlson, 2019; Uchendu et al., 2021). Furthermore, a review of published literature by Uchendu et al. (2021), as shown in Figure 4 below highlights research that has been undertaken where the information security culture, cybersecurity culture, security culture has been researched. There is a clear indication in the figure that cybersecurity culture is not adequately ventilated. This observation is further corroborated by authors stating that literature related to understanding cybersecurity culture is still in its nascency and further research is required (Alshaikh, 2020).

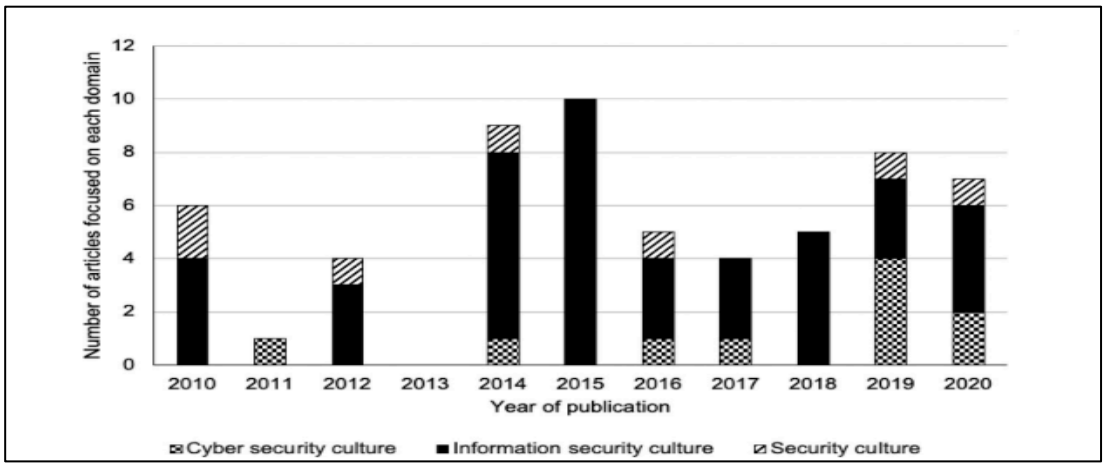



Figure 4 Distribution of Articles (Uchendu et al., 2021)

### 2.3.3 Cybersecurity Culture

Recently, scholarly research has emphasised ensuring that organisational cybersecurity culture is embedded throughout all levels of an organisation, from employees to management. Scholarly definitions describe cybersecurity culture as the beliefs, attitudes, assumptions, values, and knowledge employees use when interacting with information resources in an organisation. These influence the behaviour of the employee towards information resources within the organisation (Da Veiga et al., 2020; Georgiadou, Mouzakitis, et al., 2022a; Huang & Pearlson, 2019; Kabanda, 2018).

### 2.3.4 Cybersecurity Culture Levels

External factors are considered necessary when assessing cybersecurity in individual organisations. A prominent factor recently ventilated in academia is national and regional culture, which can be determined as the differences that determine and influence individuals towards certain cybersecurity behaviours (Gcaza & Von Solms, 2017b; Mwim & Mtsweni, 2022). Furthermore, for organisational cybersecurity to be successful, the cybersecurity culture landscape needs to be assessed beyond the organisational setting to incorporate a national and, at times, international outlook (Da Veiga, 2016). Figure 5 depicts the different levels that cybersecurity can be viewed from.

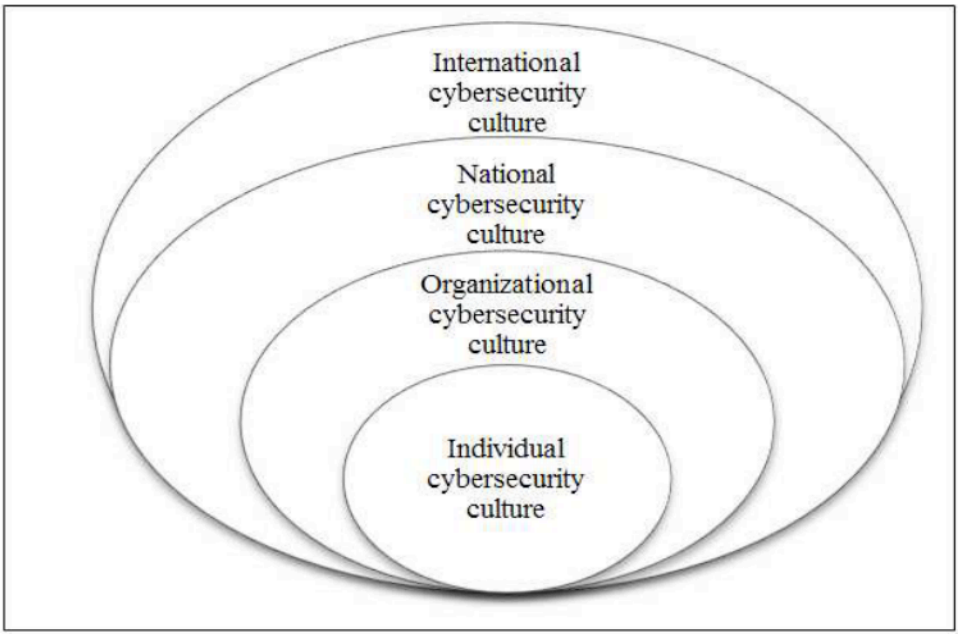



Figure 5 Cybersecurity Culture Levels (Da Veiga, 2016)

### 2.3.5 Cybersecurity Culture Factors

Although research has identified factors that promote organisational cybersecurity culture, a definite list has not been established. Nevertheless, several factors that promote a positive cybersecurity culture have been listed in academia; these include top management support, accessible policies and procedures, security education, training and awareness, psychological perspectives, and having a cybersecurity champion (Mwim & Mtsweni, 2022; Uchendu et al., 2021).

#### 2.3.5.1 Top Management Support

Management support is crucial in ensuring that cybersecurity culture is embedded across the organisation. Management support has been identified in most studies as the top factor that promotes a positive cybersecurity culture (Mwim & Mtsweni, 2022; Uchendu et al., 2021). Management support has been identified in most studies as the top factor that promotes a positive cybersecurity culture. Ultimately, top management provides the direction for the initiatives required to promote a cybersecurity culture in the organisation. Management must define the cybersecurity strategy, provide the necessary budget and ensure the organisation is adequately resourced in the security department (Mwim & Mtsweni, 2022).

#### 2.3.5.2 Accessible Policies and Procedures

Policies and procedures are the cornerstone of providing clear guidelines for the management and the boundaries of cybersecurity culture. Clear, well-articulated, and accessible policies and procedures are crucial for ensuring that the cybersecurity culture is promoted effectively within the organisation

(Georgiadou, Mouzakitis, Bounas, et al., 2022; Mwim & Mtsweni, 2022). Furthermore, developing a cybersecurity culture should start with formulating policies for all employees who handle company information (Ioannou et al., 2019).

#### 2.3.5.3 Security Education, Training and Awareness

Security education, training and awareness (SETA) is a management mechanism that is put in place to provide organisation members with the necessary, appropriate, and essential cybersecurity training and education required to effectively recognise and appropriately handle cyber-related threats and scenarios (Mwim & Mtsweni, 2022; Uchendu et al., 2021). SETA appears in most of the research undertaken in cybersecurity culture studies, making it one of the most important criteria in effective cybersecurity culture cultivation (Mwim & Mtsweni, 2022; Uchendu et al., 2021).

#### 2.3.5.4 Psychological Perspectives

As researchers have posited, beliefs, values, and attitudes (BVA) are at the core of cultivating cybersecurity culture (Georgiadou, Mouzakitis, Bounas, et al., 2022; Huang & Pearlson, 2019; Mwim & Mtsweni, 2022). However, additional psychological factors have also been cited in academia as having a significant impact on cybersecurity culture; these include trust, sharing, and ethical behaviour (Marotta & Pearlson, 2019; Mwim & Mtsweni, 2022; Uchendu et al., 2021).

#### 2.3.5.5 Cybersecurity Champion

Building a network of cybersecurity champions in the organisation is important to promote initiatives that are driven by senior management. This initiative is a collaborative effort across various management lines to promote a holistic cybersecurity culture across the organisation (Alshaikh, 2020; Mwim & Mtsweni, 2022). Having cybersecurity champions in the organisation has been cited as a major factor, as peers within the organisation can share ideas and discuss cybersecurity-related issues.

The factors listed are not all those deemed key to enabling a positive cybersecurity culture. However, they have been identified as the prominent factors in academia. Table 2, highlights literature that has identified these factors as influential in cybersecurity culture.

| Authors | Factors | | | | |
|---|---|---|---|---|---|
| | **Top Management Support** | **Policies and Procedures** | **SETA** | **Psychological Factors** | **Cybersecurity Champion** |
| Mwim and Mtsweni (2022) | X | X | X | X | X |
| Uchendu et al. (2021) | X | X | X | X | X |
| Alshaikh (2020) | X | X | X | X | X |
| Huang and Pearlson (2019) | X | X | X | X | X |

Table 2 Cybersecurity Culture Factors

### 2.3.6 Challenges of Promoting a Cybersecurity Culture

Establishing a cybersecurity culture presents problems in its effective implementation and management inside the company. Academic experts have identified difficulties through a literature review. This section will address the challenges.

#### 2.3.6.1 Lack of Management Support

Support from top management is critical in fostering an organisational cybersecurity culture. (Huang & Pearlson, 2019; Uchendu et al., 2021). However, studies indicate that top management support remains challenging in most organisations (Da Veiga et al., 2020). Understanding of cybersecurity issues and reactive top management are elements that have contributed to the lack of management support as identified in academia (Bada et al., 2018; Shillair et al., 2022).

#### 2.3.6.2 Lack of Security Education, Training and Awareness

Effective security education, training, and awareness (SETA) has been identified as a primary factor influencing a robust organisational cybersecurity culture (Alshaikh, 2020; Barlow et al., 2018; Da Veiga et al., 2020; Huang & Pearlson, 2019). However, previous studies have noted that SETA has remained

a concern, with digital labour platforms offering limited SETA to their employees (Broughton et al., 2018; Thomas & Baddipudi, 2022; Wood et al., 2019).

#### 2.3.6.3 Lack of Resources

Inadequate cybersecurity resourcing remains an issue for management (Da Veiga et al., 2020; Shillair et al., 2022; Uchendu et al., 2021). Lack of budget and skilled resources are some of the main reasons for resourcing challenges; it is also noted that resourcing is an issue for small and large organisations (Furnell & Shah, 2020; Kabanda et al., 2018; Shillair et al., 2022).

## 2.4 Gig Economy

The concept of "gig", initially posited in the music industry, is typically deemed short-term arrangements of a musical event (Woodcock & Graham, 2019), has evolved beyond its original context and is now utilised to encompass diverse sectors (Tan et al., 2021; Watson et al., 2021). These sectors include service organisations, food and beverage delivery, transportation, and other work-on-demand or crowd-work platforms (Tan et al., 2021; Wood et al., 2019). However, it should be noted that the concept of gig work or demand services has been persistent in other forms over the last few decades; this list includes minicab services, babysitters, house cleaners and many others (Tan et al., 2021; Watson et al., 2021).

Although gigs have been persistent in these sectors over time, the relatively newly established gig economy, which can be described as tasks that are digitally mediated and involve fulfilling tasks through Internet-based platforms that can either be performed online or offline (Anwar & Graham, 2021), is empowered through enhanced digital platforms and is slowly replacing traditional gigs that are not online or platform mediated (Woodcock & Graham, 2019). Furthermore, consensus on the gig economy is clarified through a wide array of published research definitions with similar fundamental concepts. Tan et al. (2021, p. 2) describe the gig economy as "markets in short-term, on-demand, occasional, and typically task-based labour". Wood et al. (2019, p. 57) define the gig economy as "people using apps (also commonly known as platforms) to sell their labour".

However, scholars also argue for the ambiguous nature of defining the gig economy. As a contestable concept, the gig economy has been argued to be a hybrid work arrangement that borders self-employment and standard employment (Montgomery & Baglioni, 2021). This concept is further explained as a juxtaposed situation where the gig economy represents opportunities, flexibility, and other benefits for individuals and others, a significant decline in job quality (Montgomery & Baglioni, 2021). Furthermore, platform-based organisations have been known to refer to gig workers as independent contractors and not as full-time employees to bypass labour practices (Barratt et al., 2020; Peterson & Steinbaum, 2023). This practice adds precarity to the gig workers as they do not reap the benefits of traditional labour practices (Anwar & Graham, 2021).

Nevertheless, due to its flexibility and remote work nature, the gig economy was the Society for Industrial and Organisational Psychology's number one trending topic for 2023 (Society for Industrial and Organizational Psychology, 2023). Participation in this industry is expected to increase drastically in the coming years. In a South African context, the gig economy is driven by urbanisation, regulations favouring entrepreneurship and innovation, high penetration of mobile phones, and connectivity infrastructure (Van Belle et al., 2023). Furthermore, over the last decade, the accelerated adoption of Information and Communication Technology (ICT) coupled with the Covid-19 2020 pandemic accelerated the wide adoption of the gig economy, particularly in emerging markets (Kuhn et al., 2021; Thomas & Baddipudi, 2022; Watson et al., 2021).

The gig economy is made up of gig workers, who are further divided into subcategories. The following section will explain these concepts further.

## 2.5 Gig Workers

Over the last decade, gig workers have been defined in several ways, including on-demand workers, short-term workers, contractual workers, freelancers, independent workers, temporary workers, and so on (Ungureanu, 2019; Vallas & Schor, 2020). However, this report defines gig workers as individuals who generally perform services through online mediated platforms, either offline or online (Vallas & Schor, 2020). The gig economy is classified into several categories, with the two primary types being cloud-based and platform-based work.

### 2.5.1 Cloud-Based Work

Cloud-based, frequently called crowd working, mainly online mediated tasks and is usually once-off, and popular platforms include Upwork and NoSweat. This line of work is mainly utilised by professionally qualified consultants, contractors or freelancers. These users provide professional services and are engaged on a project-by-project basis (Vallas & Schor, 2020). Furthermore, this work may include non-professional services like tagging pictures, transcribing text and proofreading (Tan et al., 2021).

Cloud-based work is an enduring topic of discussion, with prominent issues around the autonomy paradox being widely discussed (Kinder et al., 2019; Peterson & Steinbaum, 2023). Simply put, cloud-based work promises more flexibility and power for its users (Peterson & Steinbaum, 2023; Tan et al., 2021). However, algorithmic management platforms overshadow this flexibility and power (Anwar & Graham, 2021; Cant, 2019; Wood et al., 2019). Algorithmic management is described as a form of digital management. This form of impersonal management is known to cause tension between the workers and the platforms. Ratings, future work, reputation, and constant monitoring are some algorithmic management functions that workers see as a stumbling block when engaged in this form of work (Anwar & Graham, 2021; Tan et al., 2021; Wood, 2021b).

Cloud-based work has been described as generating a new form of precarious work arrangement, cited as contributing to the ill-treatment of cloud-based workers (Barratt et al., 2020; Tan et al., 2021). Additionally, the precarious nature of cloud-based work has led to issues around mental well-being (Apouey et al., 2020; Kim et al., 2023; Wang et al., 2022), loneliness (Anwar & Graham, 2021; Broughton et al., 2018; Wang et al., 2022), and financial constraints (Apouey et al., 2020; Wood et al., 2019).

Nevertheless, participation in cloud-based work is growing rapidly and shaping how organisations and employees interact. This new paradigm shift in the working relationship was estimated to grow rapidly in Sub-Saharan Africa between 2016 and 2020, with online job postings rising above 130% (Datta et al., 2023). Figure 6 below is a graphical illustration of the growth rate of online cloud-based job postings in the different regions.

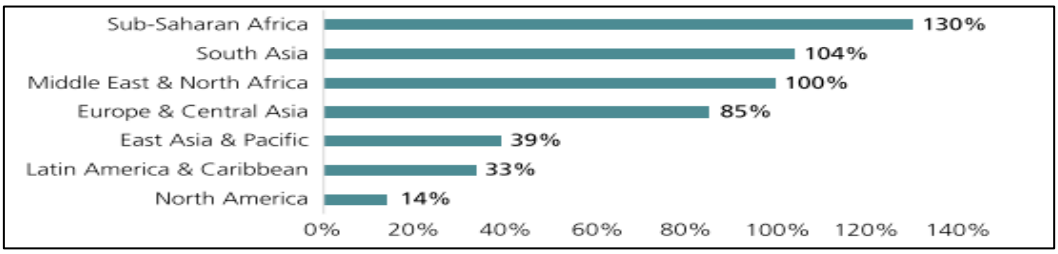



Figure 6 Growth rate of job posting from 2016-2020 based on region (Datta et al., 2023)

Despite cloud-based workers' challenges, the industry's rapid growth has been attributed to several benefits, such as flexibility and a higher earning potential.

#### 2.5.1.1 Flexibility

Flexibility is the highest-rated benefit among cloud-based workers. Shorter working arrangements and no physical work location increase flexibility in cloud-based work (Apouey et al., 2020; Datta et al., 2023; Tan et al., 2021). Flexibility also affords the cloud-based worker the ability to work on multiple jobs at the same time. However, scholars have argued that the concept of flexibility has numerous interpretations, and this is based on which side you are on. Hiring firms view flexibility as the ability to exploit labour markets to maximise profitability and also shift risks associated with having a full-time labour force (Anwar & Graham, 2021). Furthermore, firms set the price, timing of jobs, and workload allocation (Anwar & Graham, 2021; Tan et al., 2021). These factors can significantly impact workers' flexibility based on where they are. Additionally, cloud-based workers have been known to work over 40 hours a week, which does not fully represent flexibility (Datta et al., 2023).

On the other hand, cloud-based workers view flexibility as defining and controlling their own working hours, routines, and places of work (Anwar & Graham, 2021; Broughton et al., 2018; Tan et al., 2021).

Furthermore, cloud-based workers have expressed that flexibility also shields them from office politics and other issues that office-based workers may encounter (Broughton et al., 2018).

#### 2.5.1.2 Higher Earning Potential

Cloud-based work offers individuals the ability to work on multiple engagements at the same time. This ability can be translated into a higher income for the individual (Anwar & Graham, 2021; Apouey et al., 2020). However, research also indicates the precarious nature of income for cloud-based workers as they do not reap the benefits of full-time employees, such as income protection and labour laws (Apouey et al., 2020; Tan et al., 2021). The following passage will look at platform-based work, which aligns more with food delivery work.

### 2.5.2 Platform-Based Work

The second category is platform-based and includes tasks generally performed on location or offline; these include food delivery, e-hailing services, cleaning, general maintenance and more; popular platforms include Uber, Mr D and SweepSouth (Tan et al., 2021; Vallas & Schor, 2020). This category generally offers more challenges to the workers, as workers are at the mercy of the temporal demands of customers (Vallas & Schor, 2020). Figure 7 below is a graphical representation of the skill level required for crowd work and platform-based work, as well as the geographical reach.

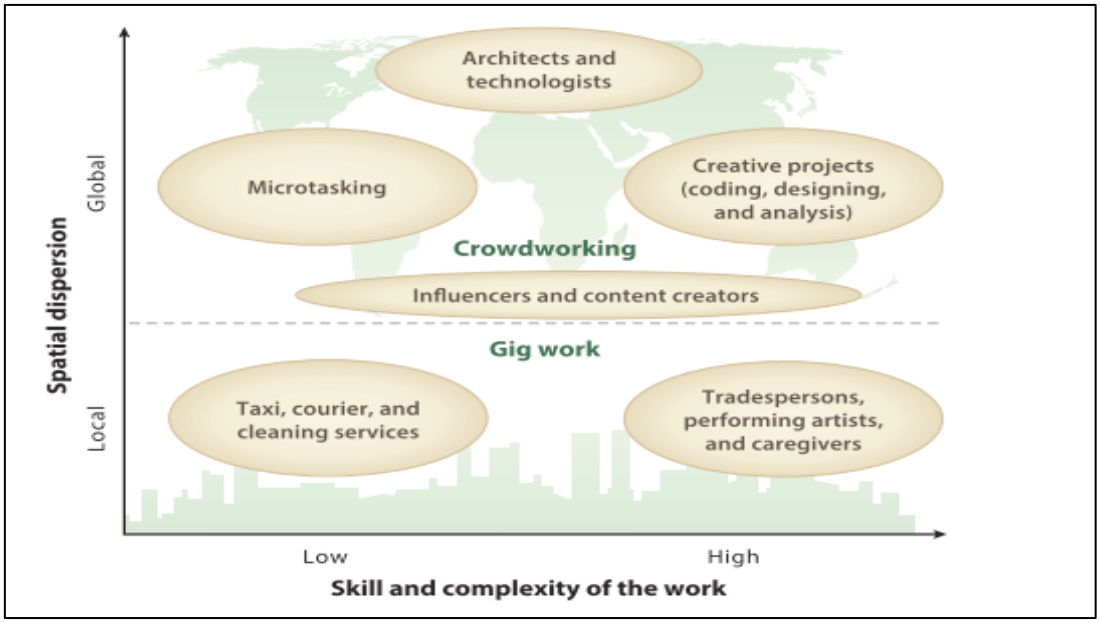



Figure 7 Type of Work and Skill (Vallas & Schor, 2020)

### 2.5.3 Platform-Based Food Delivery Work

Food delivery, a predominant subset of the gig economy, has been instrumental in driving its expansion over the last decade and has revolutionised how the economy obtains food from traditional restaurants

(Chowdhury, 2023). Several scholars have studied the sector in depth, uncovering various topics and issues. Chowdhury (2023), a study based in Bangladesh, found that convenience impacts the consumer's attitudes and behavioural intentions towards online food purchases. A study on food delivery workers in France uncovered issues around worker financial precarity, mental health issues, and safety (Apouey et al., 2020). Work conducted in Australia found that food delivery platforms designate workers as contractors, allowing them to bypass labour protections (Barratt et al., 2020). This work resonates with work conducted in South Africa, which found that workers in the food delivery sector are considered independent (Kavesa & Mbali, 2022).

Furthermore, research in the food delivery sector has explored topics around logistics (Shan & Yao, 2024), behaviours of consumers towards food delivery platforms (Chowdhury, 2023; Shankar et al., 2022), the impact of digital platforms (Veen et al., 2020). Researchers have further explored last-mile delivery challenges (Puram et al., 2021), gig work precarity (Apouey et al., 2020; Vallas & Schor, 2020), and algorithmic management (Tan et al., 2021; Wood, 2021b). The rise in the sector has also raised concerns about labour issues, health issues and the sustainability of the sector (Apouey et al., 2020; Wang et al., 2022). However, work on food delivery work and cybersecurity is still an avenue that is yet to be explored.

Several other challenges related to platform-based food delivery workers have been extensively documented (Chibanda et al., 2022). Challenges related to employee training, algorithmic management, and work precarity have also been documented (Lesala Khethisa et al., 2020). The following section will explore these challenges in greater detail.

## 2.6 Challenges of Gig Work

### 2.6.1 Employee Training

Numerous studies have found that gig economy platforms offer limited training to gig economy workers. Training needs to be more consistent as workers have reported inconsistencies concerning on-the-job training and training on company policies (Broughton et al., 2018; Wood et al., 2019). Lack of employee training has remained enduring in literature. Studies suggest that human resources in gig economy companies must adequately address the issue (Malik et al., 2021). Furthermore, it has been argued that the gig economy platforms should adequately ventilate cybersecurity policies and practices to ensure that gig workers can make informed decisions regarding cybersecurity safeguarding (Furnell & Shah, 2020).

However, this has not improved, as industry research has highlighted that platforms must inform employees about company security policies and the importance of cybersecurity (Beyond Identity, 2023). Furthermore, due to the nature of work in the gig economy, workers typically use their own devices to carry out tasks. Without adequate training on cybersecurity, this may introduce additional

security risks to the platform company. Table 3 below, highlights literature that has addressed the lack of employee training in the gig economy.

| Challenge: Lack of Training | | |
|---|---|---|
| **No** | **Author** | **Discussion** |
| **1** | Broughton et al. (2018) | Training to gig workers was inconsistent, with workers forced to source their own training and at times their own expense. |
| **2** | Ungureanu (2019) | Gig workers generally need to pay higher to compensate for the training provided to permanent workers. |
| **3** | Malik et al. (2021) | Human resource management functions such as training become obsolete when gig economy conditions are introduced. |
| **4** | Wood et al. (2019) | Firms have shifted the financial responsibility for skills development to gig workers. |

Table 3 Challenge: Lack of Training

### 2.6.2 Algorithmic Management

The term algorithmic management was first coined in 2015, and it relates to "software algorithms that assume managerial functions and surrounding institutional devices that support algorithms in practice" (Lee et al., 2015, p. 1603). It has been noted that algorithmic management techniques have been used extensively by online mediated platforms to rank employees through user ratings and preferences (Wood et al., 2019). In the past, these techniques have been found to offer many benefits to gig economy employees, like high levels of flexibility, autonomy, and complexity (Tan et al., 2021; Wood et al., 2019). However, ethical debates have also been raised against algorithmic management, which can be seen as a controlling system by the employees and a surveillance mechanism (Anwar & Graham, 2021; Vallas & Schor, 2020). Furthermore, it has been noted that gig workers have found mechanisms to manipulate the algorithms in their favour for better ratings and more work (Vallas & Schor, 2020). Table 4 below, highlights literature that has addressed challenges related to algorithmic management.

| Challenge: Algorithmic Management | | |
|---|---|---|
| **No** | **Author** | **Discussion** |
| **1** | Anwar and Graham (2021) | Even though workers in the gig economy enjoy freedom to choose the employers they prefer, workers are constrained by algorithmic controls. Furthermore, these controls influence the workers autonomy, flexibility and power. |
| **2** | Wood (2021b) | Algorithmic management may influence firms in investing less in skills, it is argued that technical enhancements like algorithmic management are assumed to be skills-biased. |
| **3** | Tan et al. (2021) | Ethical issues concerning algorithmic use are raised. The authors argue that algorithmic management may be discriminatory to social groups in terms of pricing and allocation of work. |
| **4** | Kaine and Josserand (2019) | Algorithmic management constrains workers and works in the benefit of the platform company. |

Table 4 Challenge: Algorithmic Management

### 2.6.3 Work Precarity

Work precarity is an endearing topic pervasive across several sectors but has found prominence in the gig economy (Mpofu et al., 2020). Several studies have found that platforms' reliance on independent contractors has created a precarious working relationship that circumvents traditional labour protection, disregards minimum wages, aborts provisions for sick leave, and does not guarantee job security (Bajwa et al., 2018; Barratt et al., 2020; Woodcock & Graham, 2019). This precarious working arrangement has been found to lead to issues of loneliness and mental health issues (Wang et al., 2022), financial stress (Gregory, 2021; Ungureanu, 2019), and social and economic exclusions (Pankaj & Jha, 2024; Tan et al., 2021). However, scholars have cautioned against precarity being exclusively reserved for gig-like work and argue that precarity also exists in standard traditional work (Anwar & Graham, 2021). Traditional workers also experience job insecurity through temporary contracts, outsourcing, and hour-based arrangements (Anwar & Graham, 2021).

Long-term financial instability, lack of career progression, and inadequate retirement planning remain concerns for precarious workers across traditional and gig economy workers (Bajwa et al., 2018; Kaine & Josserand, 2019). While governments and other labour organisations have attempted to address the precarious nature of gig work through legislation and social reforms, enforcement has been lacking to a large extent (Broughton et al., 2018; Tan et al., 2021).

The previous section discussed the gig economy in detail, highlighted the diverse definitions of gig work and furthermore, explored the challenges of the gig economy. The following section will look at the theoretical frameworks considered for the study.

# 3 Theoretical Frameworks

Cybersecurity culture studies have highlighted the lack of agreed upon measurement criteria for assessing cybersecurity culture within organisations. While conceptual framework proposals in academia are abundant, there is no consensus on an approved measurement framework (Uchendu et al., 2021). Furthermore, these frameworks have been criticised for being impractical to apply in practice (Dornheim & Zarnekow, 2023). Moreover, organisations have been criticised for using standard measuring tools, such as simulated phishing campaigns, as a tick-box exercise and to appease boards through data-driven reporting (Dornheim & Zarnekow, 2023). This study assessed three conceptual cybersecurity culture frameworks, namely, the Cybersecurity Culture Model (CCM) by Huang and Pearlson (2019), the Cybersecurity Culture Model by Georgiadou, Mouzakitis, Bounas et al. (2022), and lastly, A Framework for a Military Cybersecurity Culture Program (Leenen & van Vuuren, 2019).

## 3.1 Cybersecurity Culture Model

The theoretical lens adopted in this study was the Cybersecurity Culture Model (CCM) by Huang and Pearlson (2019). The framework was used to develop the initial interview guide, observation protocols, and preliminary coding schemes; however, it was not restrictive in the emergence of new insights (Bowen, 2006). The CCM was used as the foundation to inform background ideas that shaped the overall research problem and offered ways of seeing, organising, and understanding experiences, serving as starting points for building the analysis (Bowen, 2006; Zaidi, 2022). Furthermore, the sensitising concepts offered the researcher the opportunity to develop a conceptual framework that emerged from the data collection.

The conceptual model was introduced in 2019 and is particularly constructive for conducting socio-technical research. The model considers external and internal factors that shape employee BVAs, ultimately influencing cybersecurity behaviour (Huang & Pearlson, 2019). Additionally, researchers have not agreed on measurement criteria for cybersecurity culture within organisations, and the proposal of conceptual frameworks in academia is abundant, with no consensus on an approved measurement (Uchendu et al., 2021). This model's emphasis on behaviour is vital for this study as it acknowledges that employees are often the weakest link in the organisation (Huang & Pearlson, 2019; Warrington et al., 2021). Figure 8 below is a depiction of the Cybersecurity Culture Model.

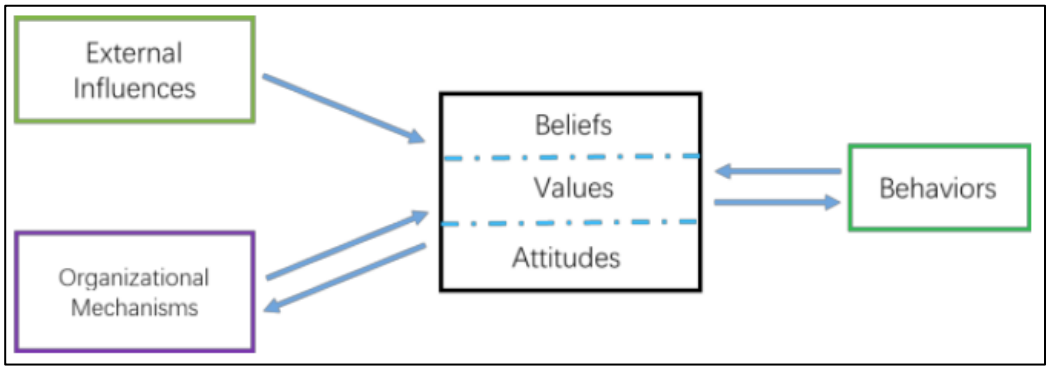



Figure 8 Cybersecurity Culture Model (Huang & Pearlson, 2019)

CCM has four constructs that will be used to sensitize and guide the data collection on the cybersecurity culture of food delivery workers in the gig economy.

### 3.1.1 External Influences

External Influences are the factors outside the organisational setting that influence the BVAs of the individual and organisational cybersecurity culture (Huang & Pearlson, 2019). External influences include national and regional culture, legislation, and peer organisations' activities (Huang & Pearlson, 2019; Uchendu et al., 2021). This construct is significant in the food delivery sector as cross-organisational interactions between the workers and media attention on the industry shape the workers' BVAs. These external factors have a direct influence on the organisation's cybersecurity culture.

### 3.1.2 Organisational Mechanisms

Organisational mechanisms are the internal factors of the organisation that promote a positive cybersecurity culture (Georgiadou, Mouzakitis, Bounas, et al., 2022; Huang & Pearlson, 2019). They are made up of various factors that include management decision-making, security, education, training, awareness, performance evaluation, rewards and punishment, and communication channels (Huang & Pearlson, 2019; Mwim & Mtsweni, 2022; Uchendu et al., 2021).

### 3.1.3 Beliefs, Values, and Attitudes

BVAs are at the centre of CCM; these three characteristics are deemed to be the organisation's unwritten rules. However, they should be observable through the organisation's leaders, groups, and individuals (Huang & Pearlson, 2019). These factors are vital for successfully promoting a cybersecurity culture (Huang & Pearlson, 2019; Mwim & Mtsweni, 2022). Furthermore, the actions of the three identified groups can be broken down into nine individual constructs, as depicted in Figure 9 below.

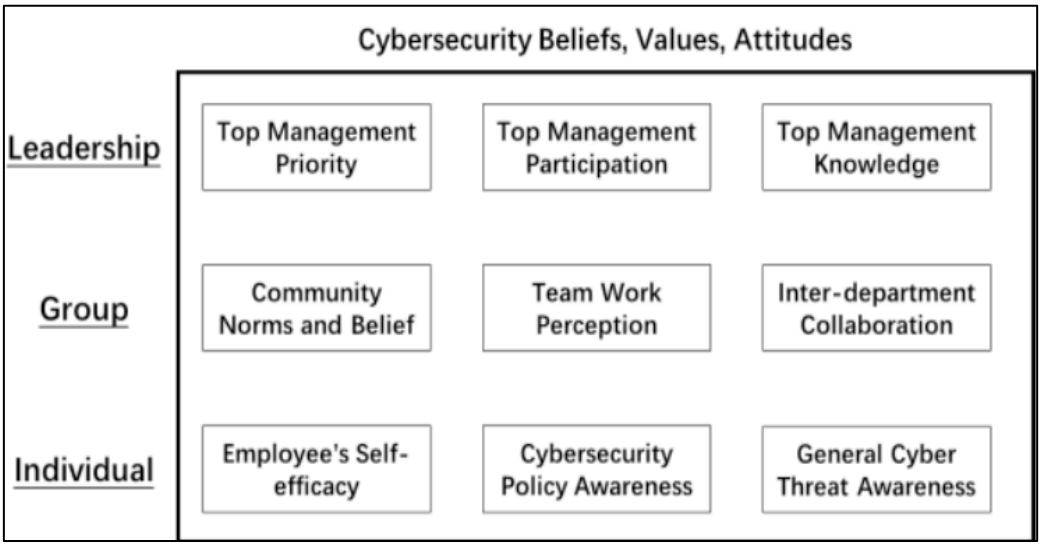



Figure 9 Cybersecurity Organisational Levels (Huang & Pearlson, 2019).

### 3.1.4 Behaviours

Behaviours are actions that ultimately reduce or create a vector for cybersecurity vulnerabilities. Behaviours also comprise in-role and extra-role behaviours, which are important in deterring cyber-related attacks (Huang & Pearlson, 2019). In-role behaviours are deemed the actions the employee partakes in to protect the organisation and are part of their job; these include compliance with policy and procedures and day-to-day security compliance (Georgiadou, Mouzakitis, Bounas, et al., 2022; Huang & Pearlson, 2019). Extra-role behaviours have been deemed as behaviours that are not part of the employee's job; these include voicing their concerns and helping others who might ask for cybersecurity-related assistance (Huang & Pearlson, 2019). Furthermore, researchers have identified the top 5 cybersecurity behaviours for organisations. Figure 10 below depicts the top 5 cybersecurity behaviours.


Figure 10 Top 5 Cybersecurity Behaviours (Alshaikh, 2020).

The Cybersecurity Culture Model by Huang and Pearlson (2019) has been used in various studies in the past. This study will adopt this theoretical lens to answer the two research questions posited as part of the study. Table 5 below summarises the studies that have applied CCM.

| Cybersecurity Culture Model (CCM) | | |
|---|---|---|
| **No** | **Author** | **Discussion** |
| **1** | Huang and Pearlson (2019) | The study was conducted using a case study on Liberty Mutual Insurance. Overall early indicators were pointing that the investments the organisation made were paying off. |
| **2** | Marotta and Pearlson (2019) | The study applied CCM to an Italian Bank, Banca Popolare di Sondrio. |
| **3** | Niu (2022) | CCM was applied to Hanshow Technology. A world leader in shelf labels and digital storage solutions. |

Table 5 Studies Using Cybersecurity Culture Model

### 3.2 Cybersecurity Culture Model

Another assessed model is the Cybersecurity Culture Model by Georgiadou et al. (2022). This model emphasises two dimensions: organisational and individual, targeting immediate impact on attributes related to security attitudes and behaviours. Although the model claims to encompass an external looking view and influence on organisational culture, it lacks an external facing dimension, which is considered important when reviewing cybersecurity culture in the gig economy. refer to Figure 11.

At an organisational level, the model comprises of six dimensions: assets, continuity, access and trust, operations, defence, and security governance. At an individual level, the model focuses on attitude, awareness, behaviour, and competency (Georgiadou, Mouzakitis, Bounas, et al., 2022). The framework proposed offers a rigorous and structured approach to evaluating cybersecurity culture within an organisation, with its core strengths being a dual layered emphasis on organisational and individual factors. However, a critical examination reveals conceptual gaps, particularly due to its omission of external factors, which limits its effectiveness as a holistic cybersecurity culture model.

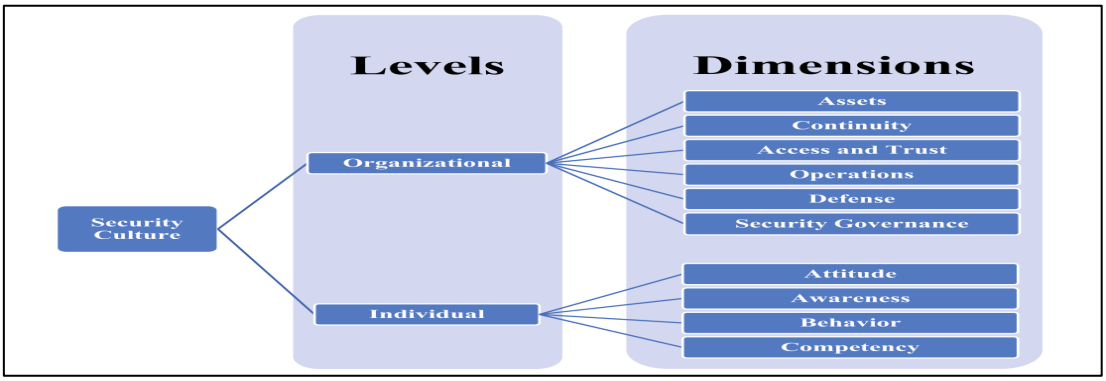



Figure 11 Cybersecurity Culture Model (Georgiadou, Mouzakitis, Bounas, et al., 2022)

### 3.3 A Framework for a Military Cybersecurity Culture Program

The final model that was considered for this study was, A Framework for a Military Cybersecurity Culture Program. However, the conceptual framework does not consider external factors and is predominately internally focused. The model's omission of external drivers and threats, as well as its over-reliance on internally facing initiatives, limits its applicability to studies that consider regional and national cultural factors. Refer to Figure 12 below.

| Preparation Phase | Design Phase | Execution Phase |
|---|---|---|
| ***a***: Cybersecurity strategy and policies must be in place | ***1***: Set up the core CSC task team | ***i***: Run awareness and educational campaigns |
| ***b***: Cyber specialists must be well trained and certified | ***2***: Define main goals, success criteria and target groups | ***ii***: Run cybersecurity exercises |
| ***c***: Understand current culture and processes, and access the risks | ***3***: Identify roles and responsibilities | ***iii***: Measure the success of the exercises |
| ***d***: : Set up an initial baseline, i.e. the current behaviours | ***4***: Identify supporting divisions | ***iv***: Return to Step 6. |
| ***e***: Run a pilot activity and measure the impact | ***5***: Design cybersecurity exercises and identify metrics | |
| ***f***: Get buy-in from upper level command | ***6***: Review and update the program | |

Figure 12 Framework for a Military CSC Program (Leenen & van Vuuren, 2019)

The model's inward-facing approach limits its potential to be applied to similar military environments in other geographical regions. The model can be enhanced by incorporating multi-level cybersecurity initiatives and integrating externally facing factors that also apply to military operations.

# 4 Research Design and Methodology

The research design and methodology followed will be outlined in the proceeding section.

## 4.1 Research Purpose

The purpose of research can be classified into various categories: exploratory, descriptive, or explanatory (Saunders et al., 2016). The purpose of this research is to be descriptive. This approach is best suited for this study as descriptive research assists in obtaining an accurate profile setting (Saunders et al., 2016).

In contrast, exploratory research is best suited to areas of novelty and new inquiries and as it asks open-ended questions to understand the research topic (Saunders et al., 2016; Swedberg, 2020; Uchendu et al., 2021). Descriptive studies are best suited for research that aims to accurately gain insights into specific events, using attitude and opinion questionnaires, as well as questionnaires on organisational practices (Saunders et al., 2016). This approach enabled the study to accurately describe the factors influencing the cybersecurity culture in the food delivery sector.

## 4.2 Research Philosophy

Research philosophy relates to the development of knowledge and the nature of the knowledge. It refers to the researcher's beliefs, which inform how the research will be conducted, including methods and approaches used in data-gathering (Saunders et al., 2016). Research philosophy is divided into two key areas: the ontological stance, which concerns the assumptions about the nature of reality, and epistemology, which pertains to what constitutes acceptable knowledge (Cunliffe, 2011; Saunders et al., 2016).

### 4.2.1 Ontology

There are two main ontological paradigms: subjectivism and objectivism. This research adopted a subjectivist ontology, which posits that reality is a social construct and a projection of human imagination. In contrast, within social sciences, objectivism sees reality as a concrete structure (Holden & Lynch, 2004). Furthermore, objectivism, at its core, is based on ontological assumptions, whereas subjectivism aims to obtain a phenomenological insight and revelation (Holden & Lynch, 2004; Saunders et al., 2016).

### 4.2.2 Epistemology

There are three distinct epistemological stances: interpretivism, critical, and positivism (Saunders et al., 2016). An interpretive paradigm allowed the researcher to gain insights from gig economy workers about the organisational cybersecurity culture, which influences their secure cybersecurity behaviour. Interpretivism is used to understand and interpret social constructs through the lens of human actors. In

its nature, it follows an emic approach (Bhattacherjee, 2012). In contrast, positivism has faced criticism for its inability to interpret real people and for overlooking the social context, which makes it unsuitable for this inquiry (Pearse, 2019). Figure 13 below illustrates the differences between philosophical assumptions.

| Assumption type | Questions | Continua with two sets of extremes | | |
|---|---|---|---|---|
| | | **Objectivism** | ⇔ | **Subjectivism** |
| **Ontology** | • What is the nature of reality?<br>• What is the world like?<br>• For example:<br>– What are organisations like?<br>– What is it like being in organisations?<br>– What is it like being a manager or being managed? | Real<br>External<br>One true reality (universalism)<br>Granular (things)<br>Order | ⇔<br>⇔<br>⇔<br>⇔<br>⇔ | Nominal/decided by convention<br>Socially constructed<br>Multiple realities (relativism)<br>Flowing (processes)<br>Chaos |
| **Epistemology** | • How can we know what we know?<br>• What is considered acceptable knowledge?<br>• What constitutes good-quality data?<br>• What kinds of contribution to knowledge can be made? | Adopt assumptions of the natural scientist<br>Facts<br>Numbers<br>Observable phenomena<br>Law-like generalisations | ⇔<br>⇔<br>⇔<br>⇔<br>⇔ | Adopt the assumptions of the arts and humanities<br>Opinions<br>Written, spoken and visual accounts<br>Attributed meanings<br>Individuals and contexts, specifics |

Figure 13 Philosophical Assumptions (Saunders et al.,2019)

### 4.3 Research Approach

This research study employed an inductive approach to analysing the data. Research approaches include inductive, abductive, and deductive (Saunders et al., 2016). Inductive approaches are employed to gain a deeper understanding of the problem, typically through the analysis of interview data collected, the formulation of a theory, and often culminating in a conceptual framework (Saunders et al., 2016). Furthermore, inductive approaches seek to establish a general understanding of the phenomena under investigation, in this case, the cybersecurity culture of food delivery workers in the gig economy (Hyde, 2000). This approach was best suited for this research, as a theory that describes the factors influencing the cybersecurity culture of food delivery workers in the gig economy has yet to be developed.

In contrast, deductive approaches, also called theory-testing, use organising frameworks and apply them to the collection and analysis of data. Furthermore, deductive approaches may aim to refine, improve, and extend existing theories (Bhattacherjee, 2012; Casula et al., 2021). The deductive research approach is predominantly associated with quantitative studies (Casula et al., 2021). Lastly, abductive approaches combine deductive and inductive approaches, where an organising framework and participation accounts are used and inform each other (Cunliffe, 2011; Saunders et al., 2016). Neither method was suited to the phenomenon under investigation.

## 4.4 Research Strategy

This study adopted a qualitative case study strategy, utilising semi-structured interviews and a qualitative research survey.

### 4.4.1 Case Study

Various research strategies can be utilised for investigation, including experiments, surveys, ethnographic research, case studies, action research, and grounded theory (Saunders et al., 2016). This research used a qualitative case study strategy. The case study strategy is best suited as it involves an in-depth inquiry into phenomena in its real-life setting (Saunders et al., 2016). A case can refer to a person, group, organisation, association, process, event, and other subjects (Saunders et al., 2016). A single case study strategy was employed for the phenomena under investigation, as no comparisons were necessary. This case study explored the experiences of food delivery gig workers in Gauteng. By utilising a case study approach, the study aimed to provide thick descriptions, and contribute to theory development (Saunders et al., 2016).

### 4.4.2 Qualitative Research

A qualitative research methodology was used in this study. Qualitative research emphasises contextual understanding and aims to comprehend the behaviours, values, and beliefs that best inform cybersecurity culture (Saunders et al., 2016). The humanistic focus is applied, as the views of the researched are applied and central to the research process (Saunders et al., 2016). Additionally, qualitative research studies meanings and the associated meanings (Saunders et al., 2016). In contrast, quantitative research is mainly associated with experimental and survey research strategies (Bhattacherjee, 2012; Saunders et al., 2016). Additionally, quantitative researchers are seen as independent from the responders, data collection is numerical and standardised, and the results are typically interpreted from the numbers (Saunders et al., 2016).

## 4.5 Data Collection

This study employed four data-gathering techniques to facilitate triangulation: semi-structured interviews, a qualitative research survey, observations, and online news articles.

### 4.5.1 Research Instruments

#### 4.5.1.1 Semi–Structured Interviews

Data were collected through semi-structured interviews with food delivery workers. The semi-structured interviews were conducted in a mixture of face-to-face and online settings (WhatsApp Calls). Semi-structured interviews are flexible; allowing the researcher to explore additional issues that may arise during the interview, and the interview can be adjusted in real time to accommodate the level of understanding of the food delivery workers (Ponelis, 2015). Additionally, a qualitative strategy is well

suited for semi-structured interviews (Saunders et al., 2016). This technique aided in providing historical and real time accounts of the phenomena under study (Gioia et al., 2013). Furthermore, during the coding analysis the initial research instrument was adjusted to probe the emergent themes from the data further. The adjusted research instrument was then utilised during the second research cycle. See; Appendix A - Semi-Structured Interview Questions and Appendix A.1 - Semi-Structured Interview Questions - Refined for the research instruments used.

#### 4.5.1.2 Qualitative Research Survey

A qualitative survey is used in social research to gain in-depth knowledge and a new understanding of social issues (Braun et al., 2021). A qualitative research survey allowed the researcher to gain more insight into the cybersecurity behaviours of food delivery gig workers in Gauteng (Jansen, 2010). The survey was administered through an online research platform approved by the university, Google Forms. Moreover, qualitative research surveys have not been used extensively in qualitative research (Braun et al., 2021). This method offered a few benefits to the researcher: it aimed to provide a wide-angle lens on the topic of cybersecurity culture in the food delivery sector of the gig economy, it provided rich and focused data, and it gave a voice to the food delivery gig workers who opted not to participate in semi-structured interviews (Braun et al., 2021). Finally, this method enabled food delivery gig workers to express their views in their own words, producing rich and complex data that encouraged discourse among them (Braun et al., 2021).

#### 4.5.1.3 Observations

Observations were employed to describe the research setting, activities, and social settings in order to gain a better understanding of the phenomenon under investigation (Saunders et al., 2016). Observations are essential when studying behaviours, as behaviours are influenced by their surroundings. Furthermore, studies have suggested an observational approach when engaging in human-centric behavioural studies, as studies that utilise questionnaires only measure knowledge and overlook behaviour (Kioskli et al., 2023; Uchendu et al., 2021). Refer to Appendix G – Observation Notes for sample notes taken.

#### 4.5.1.4 Online News Articles

Online news articles are a crucial source of written secondary data, offering timely insights and expert opinions. Several cybersecurity culture studies have utilised this data collection technique to aid in triangulation. Previous studies, such as those conducted by Gcaza and Von Solms (2017) and Senyo et al. (2024), have demonstrated how analysing media contributes to understanding the phenomena under investigation. Refer to Table 10.

### 4.5.2 Target Population

The target population was food delivery gig workers in Gauteng, South Africa. Platform-based food delivery work is an integral branch of the gig economy, with research in this area being conducted in Australia (Barratt et al., 2020; Veen et al., 2020), the United Kingdom (Cant, 2019), and China (Sun, 2019). However, there is little to no research conducted on food delivery gig workers in South Africa, Gauteng. Gauteng is the economic hub of South Africa and the fastest growing economic zone in the country and on the continent (Meyer, 2021). Moreover, Gauteng's food delivery gig work expansion has also been stimulated through government interventions, with the Gauteng Provincial Government procuring 10,000 motorcycles for the sector (TimesLive, 2023).

### 4.5.3 Sampling

Sampling is generally grouped into probability and non-probability sampling (Bhattacherjee, 2012). Probability sampling, also referred to as random sampling, has two main attributes: all items in the sample have a chance of being selected, and the selection is random. Probability sampling is not recommended for target populations of less than 50 participants (Saunders et al., 2016). In contrast, in non-probability sampling, some units in the population have no chance of being selected for inclusion. The overall number of participants considered adequate ranges from 16 and 60 (Bhattacherjee, 2012; Saunders et al., 2016). Furthermore, within non-probability sampling, there are different sampling techniques. These include quota, purposive, volunteer, and haphazard sampling.

This research employed purposive sampling as the research sampling method. Purposive sampling helped identify and select information rich food delivery gig workers for an in-depth study. Information rich food delivery gig workers provided firsthand insights and experiences relevant to the area of inquiry. Additionally, studying information rich food delivery gig workers provided firsthand insight and in-depth understanding rather than generalisations of the cybersecurity culture (Suri, 2011).

Purposive sampling is based on selecting cases directly linked to the stated research questions and objectives (Saunders et al., 2016). Additionally, homogeneous sampling was applied in this study. Homogeneous sampling emphasizes a particular sub-group where the sampled participants have similar characteristics, such as food delivery gig workers (Saunders et al., 2016). In this study, food delivery gig workers in South Africa, Gauteng, will be sampled. In contrast, heterogeneous sampling involves judgement to select a diverse range of participants (Saunders et al., 2016).

### 4.5.4 Pilot Study

A pilot study was conducted with one food delivery gig worker prior to the commencement of data collection. The pilot was also used to validate the relevance of the research instrument. The pilot study enabled the researcher to refine the questions, assess their validity and reliability, and perform a

preliminary analysis of the test pilot data to ensure the data collected could be used (Saunders et al., 2016). The pilot study comprised a semi-structured interview with one food delivery gig worker. This approach allowed the researcher to validate the instruments and refine the incoherent questions.

## 4.6 Data Analysis

Data analysis followed a cyclical approach adopted from the principles of grounded theory for inductive data analysis (Gioia et al., 2013; Turner & Astin, 2021). This analysis technique is best suited for qualitative inductive research and has been used extensively in information systems research (Alhassan et al., 2023). This method enabled interpretations to be revisited, which afforded the research more rigour and created an opportunity for the participants' point of view to be the focal point of the analysis, thereby uncovering new concepts (Gioia et al., 2013).

This approach follows a systematic cycle of open, axial, and selective coding (Alhassan et al., 2023; Saunders et al., 2016; Strauss & Corbin, 1990). Table 6 below defines the open, axial, and selective coding techniques.

| Coding technique | Definition |
|---|---|
| Open coding | *"The process of breaking down, examining, comparing, conceptualizing, and categorizing data"* (p. 61). |
| Axial coding | *"A set of procedures whereby data are put back together in new ways after open coding, by making connections between categories. This is done by utilizing a coding paradigm involving conditions, context, action/interactional strategies and consequence"* (p. 96). |
| Selective coding | *"The process of selecting the core category, systematically relating it to other categories, validating those relationships, and filling in categories that need further refinement and development"* (p. 116). |

Table 6 Coding definitions (Alhassan et al., 2023)

### 4.6.1 Data Analysis Tools

Several tools can be used for data analysis. This research employed NVivo for the data coding. NVivo is best suited for qualitative research as it can aid in research continuity, increase the rigour of the research, and transparency (Leech & Onwuegbuzie, 2011; Saunders et al., 2016).

## 4.7 Research Quality

The quality of qualitative research can be tested through validation, which involves "verifying research data, analysis and interpretation to establish their validity, credibility, and authenticity" (Saunders et al., 2016, p. 218). Two validation techniques can be used to establish quality: triangulation and participant validation (Saunders et al., 2016). This research used triangulation by implementing different data collection methods, semi-structured interviews, a qualitative research survey, observations and online

news articles. Triangulation is best suited as it adds depth, breadth, complexity and richness to the study (Saunders et al., 2016).

## 4.8 Project Plan and Timeframe

### 4.8.1 Project Plan

The research was based in South Africa, and no financial costs were incurred for the data collection phase. The only costs incurred were the researcher's petrol to travel for interviews. Meetings with the responders were pre-arranged, convenient times and locations were selected. Interviews were tracked using Microsoft Excel for record keeping and tracking. Table 7 for the master's course timeline.

| Deliverable | Start Date | End Date | Start Date |
|---|---|---|---|
| Proposal Presentation | 09/02/2023 | 13/03/2023 | Completed |
| Proposal | 09/02/2023 | 09/06/2023 | Completed |
| Management Assignment | 08/03/2023 | 06/04/2023 | Completed |
| Literature Review | 01/04/2023 | 28/04/2023 | Completed |
| Statistical Analysis Assignment | 12/05/2023 | 26/05/2023 | Completed |
| Qualitative Assignment | 29/05/2023 | 28/07/2023 | Completed |
| Research Design | 09/02/2023 | 25/08/2023 | Completed |
| Ethics Approval | 09/02/2023 | 30/08/2023 | Completed |
| Systems Thinking Assignment | 21/08/2023 | 15/09/2023 | Completed |
| Critical Reading Assignment 2 | 01/09/2023 | 28/09/2023 | Completed |
| Journal Conference Article | 09/02/2023 | 30/06/2023 | Completed |
| Data Collection | 01/02/2024 | 02/02/2025 | Completed |

| Deliverable | Start Date | End Date | Start Date |
|---|---|---|---|
| Data Analysis | 01/09/2024 | 05/02/2025 | Completed |
| Report Write-up | 01/11/2024 | 05/02/2025 | Completed |

Table 7 Course Timeline

### 4.8.2 Research Timeframe

There are two distinct research timeframes: cross-sectional and longitudinal. The research timeframe will be cross-sectional. Cross-sectional research relates to studying phenomena at a particular time (Saunders et al., 2016). Moreover, the time constraints of the Master's in Information Systems do not allow for longitudinal studies, which are usually carried out over a more extended period (Saunders et al., 2016).

### 4.8.3 Project Risks

South Africa is currently experiencing various levels of loadshedding, which can be erratic and change daily. Power cuts lead to degraded Internet connection and laptop batteries not having sufficient power. To counter this, the researcher will use an inverter during loadshedding and work from the office in extreme cases to meet project timelines.

## 4.9 Research Ethics and Confidentiality

Research ethics and confidentiality were maintained throughout the study. The research protocol was approved by the Commerce Ethics in Research Committee before data collection. It is important for ethical approval to be obtained prior to commencement of data collection. Participants provided informed consent, receiving adequate information, time to consider, and the opportunity to ask questions (Saunders et al., 2016). The consent form adhered to UCT requirements. Participant confidentiality was maintained, and data is securely stored on OneDrive with access limited to the researcher and supervisor.

# 5 Research Analysis, Findings and Discussion

This study conducted is descriptive in nature, the study seeks to understand how cybersecurity culture influences food delivery gig workers cybersecurity behaviour. Furthermore, the study aimed to understand and describe the cybersecurity cultural factors that influence food delivery gig workers cybersecurity behaviour.

To achieve the research objectives the following research questions aided the researcher in exploring the topic:

1. Primary Research Question: How does the cybersecurity culture influence the cybersecurity behaviours of food delivery gig workers?
2. Secondary Research Question: What factors influence cybersecurity culture among food delivery gig workers?

Semi-structured interviews, news articles, online publications, and a qualitative survey provided insights into the phenomenon being studied. The semi-structured interviews provided the most insight as they detailed the participants' experiences of how culture influences their cybersecurity behaviours and uncovered the main factors that influence cybersecurity culture among the participants. Online news articles provided real time, contextual understanding of the intersection between the gig economy and cybersecurity. Finally, the qualitative survey provided an opportunity for those not comfortable with the interview process to have their voices heard.

The following chapter expands on the findings based on the data-gathering techniques and the researcher's reflections and observations during the data-gathering stages. Data-gathering was divided into two stages: the first round consisted of semi-structured, open-ended interviews, and the second stage involved targeted questions refined based on the analysis of the first round of interviews. Table 8, below outlines the data sources and the data-gathering stages of the research project.

| **Case Overview and Data Sources** | | |
|---|---|---|
| **Category** | **First Research Cycle** | **Second Research Cycle** |
| **Case Study** | Platform-based food delivery workers based in Gauteng. | |

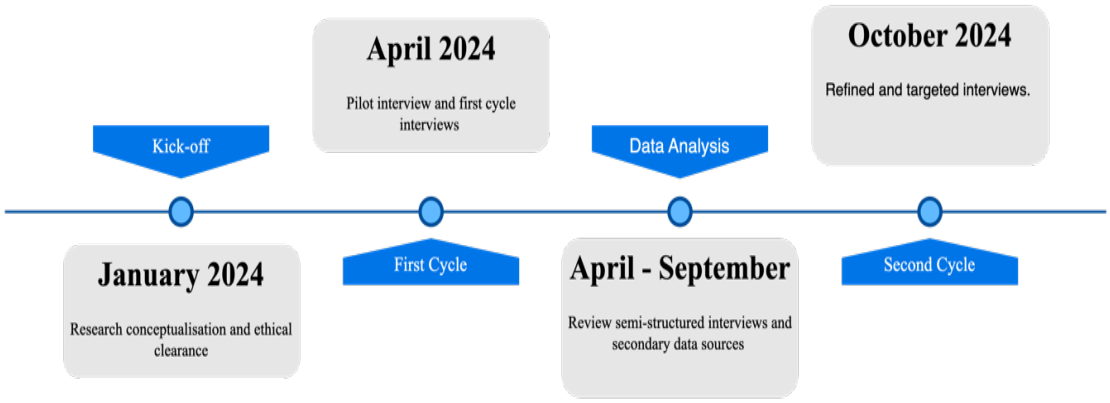
| Case Overview and Data Sources | | |
|---|---|---|
| **Study timeline:** |  | |
| **Primary Data** | 6 Semi-structured interviews. | 9 Semi-structured interviews. |
| **Secondary Data Sources** | 5 online articles<br>3 qualitative surveys | 6 online articles<br>0 qualitative surveys |

Table 8 Case Overview and Data Source

### 5.1 Background Information on Participants

Fifteen (15) food delivery gig workers were interviewed through semi-structured interviews. Of the fifteen (15) gig workers, only six (6) formed part of the first research cycle, and the remaining nine (9) were interviewed in the second research cycle. The interviews were conducted using various methods, including in-person and digital channels, such as WhatsApp calls and standard telephone calls. Table 9 below are the demographics of the participants interviewed. Three (3) of the interviewed participants have post-matric qualifications, with one having completed a Bachelor's degree in Financial Sciences. Majority have only completed high school, with a select few who did not get to complete Grade 12. The participants work for various organisations, mainly UberEats and Mr D, with several working for Checkers. The years of experience in the sector vary from four months to six years.

| ID | Food Delivery Company/s | Nationality | Education | Experience | Interview Duration |
|---|---|---|---|---|---|
| FD 1 | Mr D, UberEats, OrderIn | Zimbabwe | Form 3 (Zimbabwe). Grade 10 (SA) | 6 Years | 24 Minutes |
| FD 2 | Mr D, UberEats | Malawi | National Diploma | 2 Years | 35 Minutes |
| FD 3 | Mr D, Skida Day | Zimbabwe | 0-Level (Zimbabwe). Matric (SA) | 3 Years | 19 Minutes |
| FD 4 | Mr D, UberEats | Zimbabwe | 0-Level (Zimbabwe). Matric (SA) | 2 Years | 27 Minutes |
| FD 5 | Mr D, UberEats | Zimbabwe | N5 Mechanical Engineering | 4 Months | 31 Minutes |
| FD 6 | Checkers | South Africa | Bachelor's degree, Financial Science | 5 Months | 31 Minutes |
| FD 7 | Checkers, Mr D | Malawi | Form 4 (Malawi). Matric (SA) | 5 Years | 16 Mins |
| FD 8 | Checkers, Mr D | Malawi | Form 4 (Malawi). Matric (SA) | 4 Years | 16 Mins |
| FD 9 | Mr D | Zimbabwe | 0-Level (Zimbabwe). Matric (SA) | 1 Year | 25 Mins |
| FD 10 | UberEats | Malawi | Form 4 (Malawi). Matric (SA) | 2 Years | 25 Mins |

| ID | Food Delivery Company/s | Nationality | Education | Experience | Interview Duration |
|---|---|---|---|---|---|
| FD 11 | UberEats | Malawi | Form 4 Incomplete (Malawi). Grade 11 (SA) | 3 Months | 22 Mins |
| FD 12 | UberEats | Malawi | Form 4 (Malawi). Matric (SA) | 3 Months | 18 Mins |
| FD 13 | UberEats | South Africa | Grade 10 | 4 Months | 20 Mins |
| FD 14 | UberEats | Zimbabwe | 0-Level (Zimbabwe). Matric (SA) | 3 Months | 25 Mins |
| FD 15 | UberEats | Malawi | Form 4 (Malawi). Matric (SA) | 3 Months | 16 Mins |

Table 9 Demographics

Secondary data sources used in the research were qualitative surveys (Braun et al., 2021), and online news articles refer to Table 10 below for the online articles.

| Reference | Source | Article Title |
|---|---|---|
| Art1 | TimesLive | Gauteng government partners with UberEats to 'unlock e-commerce opportunities for township business |
| Art2 | My Broadband | UberEats of townships a massive hit |
| Art3 | Rest of World - Reporting Global Tech Stories | Need for speed: This Johannesburg driver delivers anything in 15 minutes |

| Reference | Source | Article Title |
|---|---|---|
| Art4 | Mail & Guardian | The appetite for food delivery services in townships is growing |
| Art5 | The Cyber Express | Jollibee Cyberattack: Data of 32 million customers of fast food chain allegedly compromised |
| Art6 | BusinessTech | Criminals targeting online food delivery in South Africa |
| Art7 | Techpoint.Africa | UberEats introduces new features to enhance couriers' safety in South Africa |
| Art8 | BusinessTech | Hijackers coming after these two targets in South Africa |
| Art9 | LinkedIn | Food delivery apps and data privacy concerns: protecting your information |
| Art10 | LinkedIn | Securing the digital feast: Cybersecurity in the food delivery industry |
| Art11 | Control Audits.com | What are the cybersecurity best practices for digital food delivery? |

Table 10 Online Articles

## 5.2 Coding Analysis

Open coding was applied to the data to identify first-order themes from the raw data (Urquhart, 2012). During the first and second research cycle, a comparison between emerging themes and literature on cybersecurity culture was consistently undertaken (Urquhart, 2012). Also, concurrent data analysis and collection were undertaken (Turner & Astin, 2021).

The first round of coding resulted in 18 open codes. This step was important to capture the initial sentiments of the respondents from the semi-structured interviews, qualitative research surveys, and online news articles on cybersecurity within the food delivery sector. Figure 14 below is a representation

of the first order concepts from the data. The first round of interviews was conducted with food delivery workers from January to April 2024. Appendix A - Semi-Structured Interview Questions was used for the initial data-gathering.

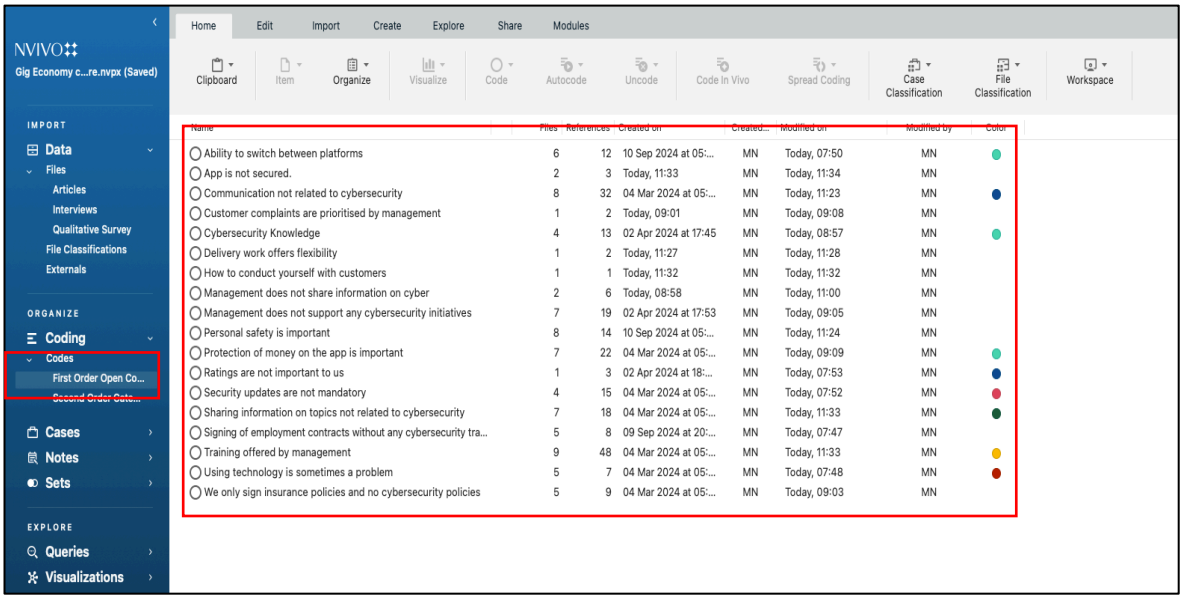



Figure 14 First-Order Concepts

Following the first round of open codes, which produced codes such as "*ability to switch between platforms,*" "*personal safety is important,*" and "*training offered by management,*" axial coding was then applied to identify connections and patterns among first-order codes (Bhattacherjee, 2012; Gioia et al., 2013; Senyo et al., 2024). This process enabled the generation of second-order themes, which provided insight into the factors that influence the cybersecurity culture and the behaviours of food delivery workers. This step produced second-order themes such as "*limited cybersecurity training and awareness*," "*management's role in cybersecurity culture*," "*information security policy implementation challenge*," "*food delivery worker safety and wellbeing*," "*platform switching and cybersecurity risks*," "*lack of application security*," and "*technology proficiency challenges*". Figure 15 below is a depiction of the second-order themes.

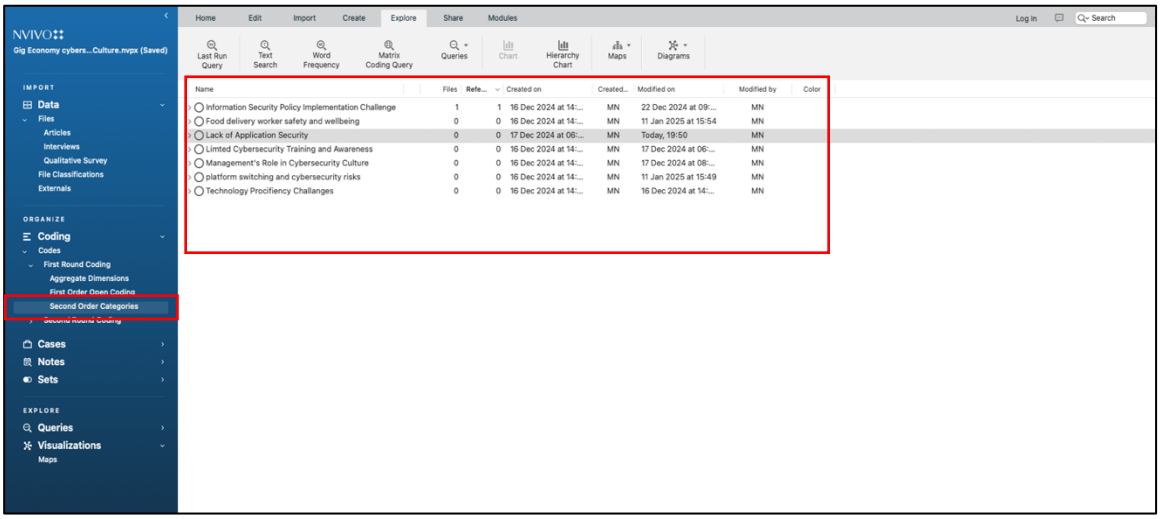



Figure 15 Second-Order Themes

Throughout the process, constant triangulation was employed by reviewing research memos; which can aid in making connections and providing clarity during the data analysis stage (Bhattacherjee, 2012; Turner & Astin, 2021). Additionally, firsthand observations were made by spending time at the pick-up spots with food delivery workers. Furthermore, informal chats with the food delivery workers were conducted while waiting for interviews. Finally, online articles were gathered throughout the research cycles. After generating second-order themes, the initial research instrument was adjusted to probe the emergent themes further from the data. The adjusted research instrument was then utilised during the second research cycle, which took place from October 2024 to January 2025; adjusting the research instrument aided in aligning the interview questions more in line with the identified themes, which aided in exploring further and provided more in-depth data collection (Turner & Astin, 2021).

Selective coding was applied to the data by aggregating the second-order themes into elevated constructs. This selective coding process enabled the identification of central categories that combine and interpret the relationships between the previously identified themes, providing a framework for understanding the factors influencing cybersecurity culture among food delivery gig workers (Bhattacherjee, 2012; Diesch et al., 2020). By combining themes such as "*limited cybersecurity training and awareness*," "*lack of management's role in cybersecurity culture*," and "*lack of information security policy implementation*". Selective coding facilitated the development of a theoretical understanding and construction of meaning regarding how these themes interact to influence cybersecurity behaviours and the broader cybersecurity culture within the food delivery gig economy. Which led to the development of a theoretical concept of "*organisational gaps in cybersecurity implementation*". Figure 16 below is an example of the process followed when conducting open coding, axial coding, and selective coding adapted from (Williams & Moser, 2019).

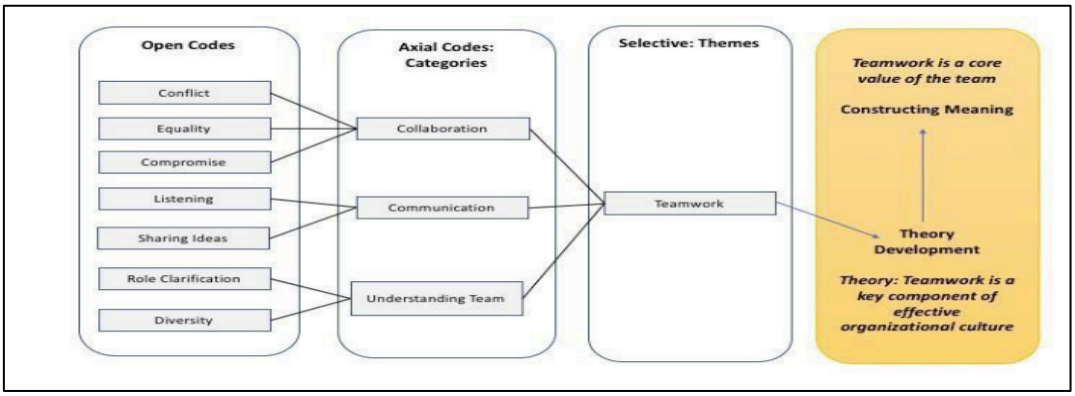



Figure 16 Creation of Theory and Meaning (Williams & Moser, 2019)

Based on the data analysis, the research unearthed three main aggregate dimensions that contributed to answering the primary and secondary research questions.

1. Organisational gaps in cybersecurity implementation
2. Food delivery worker centric needs and preferences
3. Platform-based security challenges

Appendix C – Coding Exercise and Data Structure, summarises the data analysis exercise conducted and the final data structure developed. The figure includes sample raw data from the participants, online news articles, and the qualitative survey. The data has been masked to maintain the anonymity of the participants. The following codes have been used: FD – Food delivery worker, Art – Online article, and QS – Qualitative Survey. Additionally, organisation names have been changed to maintain research confidentiality.

## 5.3 Findings

### 5.3.1 Organisational Gaps in Cybersecurity Implementation

This dimension represents the specific management and organisational factors that influence the food delivery workers' behaviours and adherence to cybersecurity practices, which answers the primary and secondary research questions:

1. How does the cybersecurity culture influence the cybersecurity behaviours of food delivery gig workers?
2. What factors influence cybersecurity culture among food delivery gig workers?

#### 5.3.1.1 Limited Cybersecurity Training and Awareness

The aggregate dimension identified includes factors that influence the cybersecurity behaviours of the food delivery workers. The first factor, "limited cybersecurity training and awareness", this factor has been identified across multiple studies as one of the contributing points to a thriving cybersecurity culture (Alshaikh, 2020; Barlow et al., 2018; Da Veiga et al., 2020; Huang & Pearlson, 2019). However,

most of the participants have cited that there is a lack of security, education, training, and awareness. For example, participant FD2 noted that there is training that takes place; however, the training is not related to cybersecurity:

> *"There is. For Org1, I'll take you to Org1 Before you start the delivery, you go, and you undergo the training. There's a form you read and answer the questions. It's a study about how to work. It touches to that security section. There's other things also, like when you are delivering alcohol and the other stuff. There's other policies also you have to know" [FD2].*

The sentiment was pervasive across most interviewed participants, as they indicated that cybersecurity-related training was unrelated. FD6, who holds a Bachelor's degree in Financial Science from one of the top universities in South Africa, indicated the following when it comes to training:

> *"The current training, they gave us on traffic signs. It's just a lot. If those that do not have licenses, they provide them with classes for that. And this time in getting licenses. And then after, that's when they gave them motorcycles to practice with. And then as soon as they're done learning, they take them through to RTT in Benoni, where they do their final test, and then when they pass, then they get granted the opportunity to start working with Org3. And then just before, they take it in. Obviously, you have to go to It's called Induction, right? Yeah, you have to go to the Induction phase where you wear all black to show that you're still in training. And then before before they can give you your own app, they first teach you how to use it. Yeah, with the other other drivers, you share trips with them, and they teach you" [FD6].*

Another worker, FD10, who has only worked with Org2, further corroborates this, indicating that their organisation offers no training at all: "*No training. No training. Because the app itself is simple. There's no any training*".

Furthermore, reviewing secondary data sources, it was noted that food delivery companies must prioritise investment in employee training and awareness. Art10 indicates that food delivery companies need to prioritise this initiative to ensure customer data is protected:

> *"Cybersecurity is not solely a technological challenge; it also involves the human element. Food delivery companies invest in employee training and awareness programs to educate staff about potential cyber threats. Training includes recognizing phishing attempts, secure handling of customer data, and adherence to cybersecurity best practices" [Art10].*

However, one organisation, Org1, has missed a golden opportunity to administer cybersecurity training for the workers, as indicated by FD5 and FD9. Org1 has an online portal where workers must undertake

online learning every couple of months. However, none of the learnings offered by management are related to cybersecurity.

> *"Yeah, they do an e-learning. There's an e-learning on the Org1. The e-learning for Org1 is 100% perfect, but they only leave the part to do with those criminals which are attacking people in the street" [FD5].*

FD9 further supported this by saying:

> *"No, when you log on to the app, you see the e-learnings. Also, there's At the same time, I think when there are time lapses as well. I think it's six months. When that time lapses, automatically it blocks your app. Then you have to check with your e-learning. It will show you; it will indicate on the app that you have to do your e-learning" [FD9].*

Through the participants' interactions, it was evident that there is a distinctive knowledge gap in understanding cybersecurity. Most participants seemed confused when asked, "Are you familiar with the following term?" Participants requested an explanation of the term, and most indicated with blank stares that they had never been taught what it is or what it relates to. FD7 asked, "*Actually, what is cybersecurity?*" This notion was further cemented through the confusion of thinking that cybersecurity relates to personal security, which revealed the study's central theme, and will be discussed later.

#### 5.3.1.2 Lack of Management's Role in Cybersecurity Culture

The second most significant factor indicative of a poor cybersecurity culture was the lack of management involvement in raising awareness and promoting a healthy cybersecurity culture within the food delivery worker sector. Top management support is one of the crucial factors in promoting an organisational cybersecurity culture (Huang & Pearlson, 2019; Uchendu et al., 2021). Without top management support, cybersecurity initiatives may not take priority over the food delivery workers' daily tasks of executing deliveries (Uchendu et al., 2021). However, through discussions with the participants, it was noted that management is not involved in promoting any cybersecurity initiatives.

Most participants indicated that although they receive messages from management, none of the communications shared are related to cybersecurity. This lack of management involvement was indicated in the first interview that was conducted, as FD1 stated:

> *"Uhm? They have never told us about it. I have not received any messages regarding cybersecurity" [FD1].*

Although management communicates with the workers, the messages shared are not related to cybersecurity or the safe use of technology. This sentiment was perfectly stated through the qualitative survey that was shared:

> *"We mostly wait for orders from management as we don't know them personally they control us from more than 1000km away distance they always communicate with us if there is a problem through WhatsApp and email" [QS1].*

FD6, who had a better understanding of cybersecurity, indicated: "*Yeah, they don't take cybersecurity seriously",* referring to the management of Org3. Lack of management support in promoting cybersecurity culture in the food delivery sector will not cultivate a cybersecurity aware community amongst the workers. This lack of participation by top management can lead to security incidents and exposure of customer data. Through the review of secondary data sources, it was noted in Art9 that several security breaches have occurred over the last few years in the food delivery sector, exposing company data.

> *"Org2: In 2020, Org2, a popular food delivery app, suffered a data breach that affected 100,000 users" [Art9].*

The lack of tone at the top harms the organisation and customers who support the platforms. Management participation in cultivating a cybersecurity aware community amongst the food delivery workers is important and should be prioritised (Huang & Pearlson, 2019).

#### 5.3.1.3 Lack of Information Security Policy Implementation

Policies and procedures are the cornerstone of providing clear guidelines for the management and the boundaries of cybersecurity culture. Clear, well-articulated, and accessible policies and procedures are crucial for ensuring that the cybersecurity culture is promoted effectively within the organisation (Georgiadou, Mouzakitis, Bounas, et al., 2022; Mwim & Mtsweni, 2022). Another issue that most participants raised was the lack of distribution of information security policies to the workers. As per the previous finding, this was also uncovered in the first and most subsequent interviews. FD1 stated:

> *"At Org1 we have a contract we have to sign before we start with our work. But during the work period there are no policies or documents sent" [FD1].*

The same observations were noted across the various organisations:

> *"No, there's no other document they give us, except we only buy a bag. That's all. There's no any other thing they give us" [FD10].*

FD6 further corroborated this: "*It's just a It was a lot of things, man. I had to go through them quickly because there was a bunch of guys in a room who were rushing you. I get the paperwork done. So I scanned through and then I just signed in."*

The participants indicated that the organisations make them sign contracts without explanation and that the documents they sign, only covers accidental damage to the motorbikes they utilise for making deliveries.

#### 5.3.1.4 Summary of Organisational Gaps in Cybersecurity Implementation

Factors identified in this dimension, like "limited cybersecurity training and awareness", the "lack of management's role in cybersecurity culture," and "lack of information security policy implementation" offered by food delivery companies create a significant gap in the adherence to cybersecurity policies and practices, which negatively influences the behaviours of food delivery workers. The gaps identified do not promote a healthy cybersecurity culture in the context of food delivery workers in Gauteng, South Africa. This finding indicates that the gaps identified in the management mechanisms utilised in the sector create a vector for data leakage and cybersecurity breaches, potentially impacting all stakeholders in the food delivery sector.

### 5.3.2 Food Delivery Worker Centric Needs and Preferences

This dimension relates to worker's needs, including safety, wellbeing, communication, and adaptability to cybersecurity practices. These factors significantly influence food delivery workers' willingness and ability to adopt secure behaviours and follow cybersecurity practices. The need for safety amongst food delivery workers may overshadow cybersecurity considerations.

#### 5.3.2.1 Food Delivery Worker Safety and Wellbeing

The BVAs are at the centre of cybersecurity culture; these three characteristics are deemed the organisation's unwritten rules. However, they should be observable through organisation's leaders, groups, and individuals (Huang & Pearlson, 2019). Through interviews, secondary data collection, and observations, most participants have indicated that management does not display any BVAs that promote a positive cybersecurity culture. Additionally, based on the participants' education level, grasping the concept of BVAs was challenging for them. However, these views were shared when presented with questions on the BVAs of management regarding cybersecurity: QS1 indicated.

> *"They only tell us on first day of working any mistakes regarding this they charge us money so we don't make errors" [QS1].*

The above statement indicates that top management priority is centred around delivery excellence and profits and not so much around secure cybersecurity practices; these values displayed by management

can potentially demotivate workers from adopting secure cybersecurity behaviours. Management BVAs were further corroborated by FD5:

> *"Yeah, but mostly the company is to make profit. Those people, they don't matter to them. They just want to continue getting- They're just to ensure that you did the job, and you get the nice ratings." [FD5].*

Some of the responders also believe that management does not prioritise them as individuals; FD10 indicated:

> *"Yeah, that's the problem. That's what they do. Once you report problems, or accidents, most of the time they block their account because they protect most their customers, not driver" [FD10].*

At the core of cybersecurity culture, it is apparent that management has not adopted cybersecurity core BVAs, which may negatively impact the behaviours of food delivery workers and their adherence to secure cybersecurity behaviours. Furthermore, the punitive measures indicated by QS1 and FD10 can destroy trust and lead to non-reporting of cybersecurity incidents, as the workers may deem this a punishable offence.

#### 5.3.2.2 Platform Switching and Cybersecurity Risks

Another issue identified is the workers' ability to switch between platforms and the flexible nature of the job, which introduces additional cybersecurity risks to the platforms. The constant switching between platforms has the potential to expose food delivery workers to inconsistent cybersecurity controls, which may lead to data leakages and unauthorised access to company and customer data. Several food delivery gig workers highlighted the ability to switch between platforms; FD1 indicated:

> *"I started at Org1, and then I worked at Org4 and then I moved to Org2, and now I am back at Org1 again" [FD1].*

A similar platform switching pattern was noted in the interview with FD4; they indicated that their profile for Org1 was blocked and that they were using another worker's account for Org2.

> *"For now, I'm using Uber because my account is closed"*
>
> *"I'm not using my Uber"*
>
> *"My papers are expired, so I have to submit. I did submit yesterday" [FD4].*

The evident leadership and cybersecurity training gap in the food delivery sector has exposed companies to poor data governance practices and may lead to unintended data leakages (Uchendu et al., 2021).

Furthermore, the ability to switch between platforms at any time for the workers creates a detachment in adhering to specific cybersecurity secure behaviours coupled with the lack of reinforcement cybersecurity training and education. It was noted through discussions and observed with several of the workers that cybersecurity protocols on the platforms are not consistently aligned with industry best practices; research further suggests that a lack of a cybersecurity culture may lead to weaknesses, such as the implementation of robust password management (Georgiadou, Mouzakitis, Bounas, et al., 2022). FD6 indicated that they share a PIN for logging onto the application, which may lead to the account being compromised.

> *"No, it's terrible because we all use the same pin to log in, but it's different usernames. But it's easy to catch because I can't share with you now, but if you will, can we check that somebody, no details like that, their names and their names. You can be able to make up a username for them and then just open because the password doesn't say" [FD6].*

Poor password management is pervasive across platforms and creates conflicting priorities; one worker indicated that they do not have a password because they can access orders quickly, FD11 indicated.

> *"But sometimes because this app is not allowed, sometimes to put password. Because when the order is ringing, sometimes if you put a password, when you are busy with password, order sometimes is going to go" [FD11].*

This sentiment was further observed with FD12 when they stated: "*I don't put my password on my phone*". When probed further, FD12 indicated:

> *"Yeah. It happened to my brother in Kempton Park. His phone, it was having four passwords, one phone. So, he got a heart failure. He fell. So, people who were around there, for them to use the phone, to find his relatives, it was so hard because of the phone. They I went to the people that they used to flush the phone, like Tuguia, to flash the phone so that they can get access to the phone". [FD12]*

Through observations, it was noted that phones were not secured with any authentication mechanisms. In one interaction, the researcher observed a worker handing over their device to a fellow worker to deliver on their behalf. This practice goes against good cybersecurity behaviour and can be addressed through training and awareness programs.

#### 5.3.2.3 Summary of Food Delivery Worker Centric Needs and Preferences

Factors identified in this dimension, such as "*food delivery worker safety and wellbeing*" and "*platform switching and cybersecurity risks*," significantly influence the cybersecurity behaviours of food delivery workers, such as secure password management, observing the actions of leadership and the

external influences of peer organisations (Huang & Pearlson, 2019). These factors negatively shape food delivery workers' BVAs. Furthermore, these factors highlight workers' competing priorities where immediate safety, such as job security and operational needs like, customer satisfaction often overshadow secure cybersecurity practices.

### 5.3.3 Platform-Based Security Challenges

The final dimension focuses on the challenges food delivery workers encounter when using food delivery platforms, such as inadequate application security, a lack of regular updates, and the workers' varying levels of technological proficiency.

#### 5.3.3.1 Lack of Application Security

Inadequate management interventions and cybersecurity culture leadership in the food delivery sector have raised concerns about the security of applications being utilised by workers. Georgiadou, Mouzakitis, Bounas et al. (2022) found that organisational dimensions such as assets, access and trust, and security governance play a significant role at the managerial level in fostering cybersecurity culture.

Throughout the interviews, several vulnerabilities were discussed with the workers who were using the applications. FD5 indicated that the application is acquired from one worker to another.

> *"Mostly the app, we get it via ShareIT. Like me, the app in my phone, I can transfer it to your phone. That's how it works. When they bring a new version, we'll get it also through same way because it's not on Play Store" [FD5]*

FD6 further corroborated that security settings on their phones must be adjusted for the application to function. The two workers work for different platforms:

> *"I I'm really not sure because even the app that we're using, it's not even licensed to be available on a Google Play Store. You have to receive it through. What are these things? Share it. It's an app that shares apps from other phones. And then you have to turn off some stuff on your phone for it to be able to to operate" [FD6].*

The lack of management initiatives to establish a cybersecurity culture in the food delivery sector has resulted in significant gaps in the security of the applications utilised by the workers. This gap in cybersecurity controls has created the impression that it is not a priority for top management in the food delivery sector. Workers have also expressed the belief that management prioritises profit making over other activities, a sentiment supported by the apparent gap in security controls. Additionally, interviews with workers uncovered that security updates are not mandatory on these platforms, a concern raised by several participants.

FD5 indicated that since he started using the application, he has never updated it: "*Yeah, you can still use it. I've never It's been updated since I started using it.*". This was further corroborated by FD6 and FD7.

> *"Yeah, for you to be able to use the app. Oh, okay. And then- It's just one version throughout. They don't send you. We don't get an update on that app." [FD6]*

> *"I just experienced Org1 when they're updating, they just update themselves that side." [FD7]*

#### 5.3.3.2 Technology Proficiency Challenges

The study found that varying levels of technological proficiency among food delivery workers also contributed to the lack of cybersecurity practices. Most of the interviewed workers lack the technical knowledge to identify a security threat, understand why security updates are required, and use secure methods like pins or passwords on their phones. Several workers indicated that they share their accounts among themselves. Sharing accounts involves sharing sensitive data like login details, passwords, and customer information.

FD4 indicated that he sees nothing wrong with sharing account information:

> *"Somebody can use your account, you understand? If I know your pin, I can log in. When you are off or you're not working those things, I can use your account. Okay." [FD4]*

Similar sentiments were shared by FD5:

> *"But you know what- Just sometimes if you have a problem, your friend can complete your delivery. But sometimes a motorbike can have a problem. I'll say, my friend, go with my phone and deliver and bring it." [FD5]*

This sharing of information like accounts and deliveries is exacerbated by the lack of clearly structured training and awareness programs and guidance from top management. As a result, workers are granting access to sensitive information to fellow workers because they do not understand that it goes against cybersecurity practices.

## 5.4 Discussion

The following section aimed to discuss and explain the findings raised in the previous section, as well as their connection to the theoretical lens applied in the study. Furthermore, this section expands on how the findings address the research objectives and, how the objectives answer the research questions. The study's objectives were to determine how cybersecurity culture influences the cybersecurity behaviours of food delivery gig workers. The research further aimed to describe the cybersecurity cultural factors, that influence the cybersecurity behaviour of food delivery gig workers.

### 5.4.1 Summary of Research Findings

The study found the following factors significantly influence the cybersecurity behaviours of food delivery workers: organisational gaps in cybersecurity implementation with subcategories, limited cybersecurity training and awareness (Gcaza & Von Solms, 2017a; Georgiadou, Mouzakitis, et al., 2022b; Huang & Pearlson, 2019; Sutton & Tompson, 2024), and lack of management's role in cybersecurity culture (Mwim & Mtsweni, 2022; Sutton & Tompson, 2024). The mentioned factors negatively influence the cybersecurity culture, leading to behaviours that do not promote a cyber secure ecosystem for food delivery workers.

The second significant factor uncovered was the needs and preferences of food delivery workers, including subcategories related to food delivery worker safety and wellbeing. The needs and preferences of food delivery workers directly influence their BVAs (Huang & Pearlson, 2019). The phenomenon of platform switching and the associated cybersecurity risks have exposed a tendency among food delivery workers to refrain from engaging in robust cybersecurity behaviours. This reluctance is attributed to the pursuit of convenience and lack of knowledge regarding secure security practices. Previous studies have also shown that workers prioritise their needs over cybersecurity controls (Karjalainen et al., 2020; Torres & Crossler, 2024). Additionally, internally focused environments or those perceived as more professional tend to influence positive cybersecurity culture behaviours substantially (Karlsson et al., 2022).

The final factor to be discussed in this section is that Inadequate management interventions and cybersecurity culture leadership have led to concerns in the implementation of secure applications, as also discussed by Georgiadou et al. (2022). Additionally, the study found that technological proficiency contributes to workers adopting secure security practices. Previous studies have found that cognitive beliefs and workers' understanding of cybersecurity significantly influence compliance with cybersecurity control mechanisms (Onumo et al., 2021). The following section will discuss the two research questions in detail as outlined by the theoretical lens the study has adopted.

### 5.4.2 Organisational Gaps in Cybersecurity Culture Implementation

Huang and Pearlson (2019) describe external influences as significantly shaping the BVA of individuals and organisations regarding cybersecurity. In addition to the above, Huang and Pearlson (2019) further outlines that external factors significantly impact the organisation's culture. However, this research's findings indicate a significant lack of peer organisational influence on the cybersecurity culture within the food delivery sector. Food delivery companies appear to operate in silos, unlike traditional companies such as banks and insurance companies that are forced to establish best practices and foster a formalised cybersecurity culture collectively. This silo mentality has resulted in inconsistent cybersecurity practices and implementation.

The context in which this study is set, also plays a significant role as societal cybersecurity culture influences individuals' and organisations' BVAs (Huang & Pearlson, 2019; Mwim & Mtsweni, 2022). Gcaza et al. (2017) found that South Africa has concentrated on cultivating a national cybersecurity culture. This concentration aligns with several developed nations (Gcaza et al., 2017). However, this study has found that neither the national nor regional cybersecurity cultures in South Africa have had an impact on the food delivery sector in Gauteng. Furthermore, the diverse mixture of participants interviewed in the study indicates that cultural diversity at the organisational level further complicates compliance with cybersecurity practices.

#### 5.4.2.1 Limited Cybersecurity Training and Awareness

The study's findings indicated that a lack of cybersecurity training and awareness has primarily contributed to the participants' limited knowledge. These findings align with Huang and Pearlson's (2019) description of organisational learning, which states that it "*builds and retains cybersecurity knowledge*". As the platforms' primary users, the food delivery workers lack the knowledge and skills to identify and mitigate against cybersecurity threats. Training programs in the food delivery sector, when present, often lack a necessary cybersecurity focus or are focused on customer service. As a result, food delivery workers are not equipped to deal with cybersecurity threats, which increases the risk of data breaches for food delivery companies. This finding resonates with previous studies conducted by (Amoresano & Yankson, 2023; Da Veiga et al., 2020; Kangapi & Chindenga, 2022).

This lack of focused training and awareness has a negative impact on food delivery workers, as they are not adequately equipped to identify threats when they occur. Furthermore, through interactions with participants, it was also evident that the lack of training and awareness, has made breaches possible, as participants do not employ security mechanisms like password protected devices. Cybersecurity training and awareness programs should be viewed as management's intentional efforts to direct the food delivery workers to cyber-secure behaviours, which will in turn, help protect organisational assets and data.

#### 5.4.2.2 Lack of Management's Role in Cybersecurity Culture

Numerous studies have indicated that top management support is a prerequisite for a thriving cybersecurity culture (Mwim & Mtsweni, 2022; Sutton & Tompson, 2024; Uchendu et al., 2021). However, the lack of management support in the food delivery sector further exacerbates the lack of cybersecurity culture. Top management in the food delivery sector in Gauteng has not demonstrated a commitment to embedding a cybersecurity culture. This lack of commitment has led to a culture where cybersecurity controls are often an afterthought rather than a priority. Previous studies have noted that management in the gig economy prioritises profit making as one of their strategic priorities (Vallas & Schor, 2020; Woodcock & Graham, 2019). However, profit making requires the platform to exercise

more direct control over its workers, as discussed in previous literature by Anwar and Graham (2021) and Vallas and Schor (2020). As highlighted, this approach depends on data to evaluate the workers' performance.

Furthermore, the top management of the gig economy adopts an innovation-oriented management style (Butler & Brown, 2023; Sutton & Tompson, 2024). This externally focused management style prioritises flexibility to stay competitive in the market. While this approach fosters innovation and growth, it can harm platform cybersecurity practices. In the context of this study, this innovation-orientated management style has resulted in poorly structured, internally focused cybersecurity practices. This management style is evident in the responses received from the participants, as cybersecurity implementation is inconsistent and treated as an afterthought, while profit making is seen as a priority. As previously discussed, these competing priorities have led to food delivery workers receiving limited to no cybersecurity training and awareness. This results in the platforms being susceptible to cybersecurity breaches due to poor top management involvement. Since food delivery companies are externally focused and rely on contract workers to carry out food delivery tasks, management should consider the factors below identified by Willie (2023) for companies in an outsourced arrangement.

The following table, Table 11 highlights the key considerations, including shared values and expectations with outsourced partners. Clear communication channels with all parties and communication related to cybersecurity are significantly lacking in the food delivery sector. Clear communication aligns with previously mentioned findings by Huang and Pearlson (2019). The relationship between the food delivery workers and the companies is purely contractual, and no collaboration and coordination were noted. Contractual and cybersecurity obligations should be embedded in the contracts; this was also found to be lacking. Ongoing monitoring and auditing: If this had been implemented, the glaring gaps in the implementation of security protocols would have been addressed, and continuous monitoring would have been established.

| | |
|---|---|
| Shared Values and Expectations | The organization and the outsourced partners should share common values and expectations regarding cybersecurity. This includes a mutual understanding of the importance of security, compliance requirements, and the need for proactive risk management. |
| Clear Communication | Open and transparent communication channels should be established to facilitate the exchange of information related to cybersecurity. This includes sharing security policies, incident response procedures, and any relevant threat intelligence to ensure all parties are well-informed. |
| Collaboration and Coordination | Collaboration and coordination between the organization and outsourced partners are essential to address cybersecurity challenges effectively. This can involve joint training programs, periodic security assessments, and regular meetings to discuss security issues and updates. |
| Contractual Obligations | Contracts and service-level agreements (SLAs) should explicitly address cybersecurity responsibilities and expectations. The outsourced partners should adhere to the organization's cybersecurity policies and procedures, as well as comply with relevant industry regulations and standards. |
| Ongoing Monitoring and Auditing | Regular monitoring and auditing of the outsourced partners' cybersecurity practices should be conducted to ensure compliance and adherence to established security standards. This helps identify any potential vulnerabilities or gaps that need to be addressed promptly. |
| Continuous Improvement | A culture of continuous improvement should be fostered, encouraging all parties to regularly assess and enhance their cybersecurity measures. This can involve sharing best practices, and lessons learned from security incidents and implementing feedback mechanisms for ongoing improvement. |

Table 11 Key Considerations in an Outsourced Model (Willie, 2023)

#### 5.4.2.3 Lack of Information Security Policy Implementation

The study found that implementation of the information security policy (ISP) for workers is non-existent. It was noted that food delivery workers have not been made aware of ISPs or the existence thereof. Huang and Pearlson (2019) noted that in strong cybersecurity cultures, the organisation fosters an environment that strives to make employees understand ISPs and their direct influence on their jobs. This issue is consistent with numerous studies that have identified ISP implementation as having a direct influence on employee behaviours (Georgiadou, Mouzakitis, et al., 2022a; Mwim & Mtsweni, 2022; Onumo et al., 2021).

This gap in ISP implementation addresses the primary research question, primarily focusing on the effects of cybersecurity culture on the behaviours of food delivery workers. The identified gap in ISP implementation negatively influences the workers' BVA, which in turn has negatively impacted cybersecurity compliance among the workers and the organisation as a whole.

### 5.4.3 Food Delivery Worker Centric Needs and Preferences

BVAs are at the centre of CCM, these three characteristics are deemed the organisation's unwritten rules. However, they should be observable through the organisation's leaders, groups, and individuals (Huang & Pearlson, 2019). The study found that the worker's needs for safety and wellbeing have

shaped their BVA, which in turn has directed their behaviours towards cybersecurity practices. These competing priorities for safety and the ability to switch between platforms have led to a misalignment between the food delivery workers' immediate priorities, and the need to adopt secure cybersecurity practices. This misalignment is also compounded by a lack of management involvement, inadequate training, and a lack of ISP knowledge.

Most responders saw cybersecurity practices as laborious and cumbersome compared to their delivery work tasks. This observation aligns with a study by Van Der Kleij (2022), which found that users' goals to complete tasks often take priority over security controls (Van Der Kleij, 2022). Food delivery companies need to focus on user-centred cybersecurity designs, which can lead to practical and usable controls that focus on the needs and behaviours of food delivery workers (Van Der Kleij, 2022).

Furthermore, this tension between the food delivery workers' competing priorities and cybersecurity practices is shaped by the flexible nature of the work. The ability to maximise earnings (Anwar & Graham, 2021; Apouey et al., 2020), flexibility (Apouey et al., 2020; Datta et al., 2023; Tan et al., 2021), and autonomy (Wood et al., 2019) have influenced the behaviour of food delivery workers towards secure cybersecurity practices.

### 5.4.4 Platform-Based Security Challenges

A study by Georgiadou, Mouzakitis, Bounas et al. (2022) found that organisational dimensions, such as assets, access and trust, and security governance, play a significant role at the managerial level in fostering a cybersecurity culture. The lack of top management involvement in the food delivery sector has highlighted a critical issue, i.e. inadequate application security on the platforms used by food delivery workers. This finding aligns with Georgiadou, Mouzakitis, Bounas et al. (2022), who found that a lack of management involvement may lead to insecure application development. This risk exposes the food delivery workers, customers, and the organisation to vulnerabilities, data breaches, and potential fraud (Willie, 2023). This identified issue corroborates the top-down approach required to foster a cybersecurity culture (Alshaikh, 2020; Mwim & Mtsweni, 2022; Uchendu et al., 2021). Management should actively embed themselves in all levels of cybersecurity, ensuring the integration of security is prioritised and entrenched in the applications utilised. Moreover, management should consider designing training programs for middle managers and food delivery workers. This program should attempt to cultivate a shared understanding, thereby fostering a culture of cybersecurity within the sector. Alshaikh (2020) recommends embedding cybersecurity champions to assist in amplifying awareness of security, which can help cultivate a cybersecurity culture.

This chapter explored key themes emerging from the analysis of cybersecurity practices within the food delivery sector. Themes such as gaps in communication, where topics unrelated to cybersecurity dominated among the workers, and inconsistencies in training were also identified as significant

concerns. Additionally, many of the interviewed participants signed employment contracts and company policies without receiving any cybersecurity training, underpinning a reactive rather than proactive approach to risk awareness. Work flexibility and individual motivations such as, higher earning potential and personal safety, were identified as critical in shaping the behaviours of food delivery workers regarding cybersecurity practices.

Furthermore, broader goals, such as financial responsibilities and convenience, were found to intersect with cybersecurity compliance, indicating that individual and organisational priorities do intertwine and should be merged to foster greater security compliance. This chapter discussed in detail, the complexity of cybersecurity culture in the context of food delivery workers, highlighting the need for tailored interventions that consider both the individual and organisational drivers. This discussion sets the tone for the next chapter, which explores theoretical and practical recommendations designed to bridge the identified gaps and enhance cybersecurity culture within diverse workplace environments.

# 6 Conclusion

Over the past decade, cybersecurity concerns have persisted, with regular and widespread cyberattacks due to the growing sophistication of threat actors (Kravchenko et al., 2024; Sutton & Tompson, 2024). These threat actors pose significant risks to nations, organisations, and individuals, potentially impacting everything from personal data to critical infrastructure (Sutton & Tompson, 2024). However, cybersecurity controls focus on technical controls and lack frameworks that integrate cybersecurity culture into defence mechanisms (Sutton & Tompson, 2024).

This study examined the impact of cybersecurity culture on the cybersecurity behaviours of food delivery workers in Gauteng, South Africa. The findings from the study indicate that a lack of management initiatives to foster a cybersecurity culture has directly influenced the food delivery workers' secure security behaviours. Key organisational gaps, such as limited cybersecurity training and awareness, the lack of management's role in cybersecurity initiatives, and inadequate information security policy implementation, were identified as contributors to non-compliance with cybersecurity practices. These factors have significantly contributed to negative cybersecurity behaviours among food delivery workers.

Furthermore, the study uncovered a conflict between food delivery workers' safety needs, the ability to switch platforms, and adherence to secure cybersecurity practices. This misalignment highlights the challenges food delivery workers face when carrying out their tasks, particularly in terms of security requirements for secure cybersecurity behaviours.

## 6.1 Theoretical Implications

This study's findings describe how a lack of cybersecurity culture can negatively influence compliance to secure cybersecurity practices. This observation is consistent with the findings by Alshaikh (2020) and De Veiga et al. (2020). The findings contribute to the cybersecurity literature by demonstrating how the structural challenges of the gig economy, such as weak management oversight due to contractual arrangements, limited security governance, and inadequate technology proficiency, hinder cybersecurity compliance. Moreover, previous studies emphasise how external and managerial factors influence BVAs in fostering secure cybersecurity behaviours (Huang & Pearlson, 2019). This study expands the argument by demonstrating how the silo mentality prevalent in the food delivery sector weakens these factors. The apparent lack of management related mechanisms has contributed to the significant non-compliance with secure cybersecurity behaviours.

The study also contributes to theories on security, awareness, education, and training by linking non-compliance with cybersecurity practices to a lack of formal education. This observation aligns with previous studies that have found that security programs must be tailored to an organisation's needs to be impactful and empower non-technical workers (Keshvadi, 2023). Lastly, by showing that food

delivery workers prioritise financial incentives, and safety over cybersecurity practices. The study highlights the need for cybersecurity culture models that account for precarious work environments, such as the gig economy.

### 6.2 Practical Implications

From a practical standpoint, the findings suggest that food delivery platforms adopt stronger governance frameworks. The lack of clear information security policies and management cybersecurity interventions indicates a lack of strategic prioritisation. Secondly, food delivery companies should consider integrating information security policy distribution as part of their onboarding or contract-signing activities. This process will ensure that food delivery workers are aware of information security policies and promote policy compliance. This recommendation aligns with previous studies that suggest that different organisational levels may require distinct strategies for improved information security policy compliance (Balozian et al., 2019; Keshvadi, 2023). Additionally, food delivery companies should integrate security, education, training, and awareness into their applications and provide regular training through the platforms, making it mandatory for workers to complete and continue using the applications. Lastly, food delivery companies should invest in a user-centric security approach, ensuring that security mechanisms do not disrupt work efficiency, which could discourage compliance.

### 6.3 Limitations and Future Research

This study focused on the cybersecurity culture of food delivery workers in a specific regional context, precisely, South Africa, Gauteng. Despite its contributions, this study has certain limitations. While it focuses on food delivery workers within a specific regional context, it provides a foundation for understanding cybersecurity behaviours in the gig economy. However, regional and national cybersecurity cultures may influence how cybersecurity is perceived and implemented across different locations. As a result, future research should explore similar factors in other geographical areas and gig economy sectors to assess the broader applicability of these findings.

Secondly, the research does not provide insight into the views of platform providers on shaping cybersecurity culture. Future studies could investigate how platform companies, rather than just food delivery workers, influence cybersecurity culture through their management initiatives that may have been overlooked in this research.

Lastly, the study revealed that management and food delivery workers continuously reinforce a personal safety culture. Future research could investigate how personal safety can be integrated with secure cybersecurity behaviours to foster a positive cybersecurity culture.

# 7 References


Abdillah, R., Shukur, Z., Mohd, M., & Murah, T. M. Z. (2022). Phishing classification techniques: A systematic literature review. *Ieee access*, *10*, 41574-41591. https://doi.org/10.1109/ACCESS.2022.3166474

Alhassan, I., Sammon, D., Daly, M., Wibisono, A., Kasraian, L., Nagle, T., Heavin, C., Dennehy, D., Zamani, E., & Qaffas, A. (2023). The use of open, axial and selective coding techniques: A literature analysis of IS research. https://aisel.aisnet.org/ukais2023

Ali, M. M., & Mohd Zaharon, N. F. (2024). Phishing—A cyber fraud: The types, implications and governance. *International Journal of Educational Reform*, *33*(1), 101-121. https://doi.org/10.1177/10567879221082966

Almarhabi, K., Bahaddad, A., & Alghamdi, A. M. (2023). Security management of BYOD and cloud environment in Saudi Arabia. *Alexandria Engineering Journal*, *63*, 103-114. https://doi.org/10.1016/j.aej.2022.07.031

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & security*, *98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Amankwa, E., Loock, M., & Kritzinger, E. (2022). The determinants of an information security policy compliance culture in organisations: the combined effects of organisational and behavioural factors. *Information & Computer Security*, *30*(4), 583-614. https://doi.org/10.1108/ICS-10-2021-0169

Amoresano, K., & Yankson, B. (2023). Human Error-A Critical Contributing Factor to the Rise in Data Breaches: A Case Study of Higher Education. *HOLISTICA–Journal of Business and Public Administration*, *14*(1), 110-132. https://doi.org/10.2478/hjbpa-2023-0007

Anwar, M. A., & Graham, M. (2021). Between a rock and a hard place: Freedom, flexibility, precarity and vulnerability in the gig economy in Africa. *Competition & Change*, *25*(2), 237-258. https://doi.org/10.1177/1024529420914473

Apouey, B., Roulet, A., Solal, I., & Stabile, M. (2020). Gig workers during the COVID-19 crisis in France: financial precarity and mental well-being. *Journal of urban health*, *97*(6), 776-795. https://doi.org/10.1007/s11524-020-00480-4

Ashrapova, L., & Apsilyam, N. (2025). CYBERSECURITY IN THE DIGITAL ECONOMY: NEW CHALLENGES AND SOLUTIONS. *INTERNATIONAL SCIENTIFIC-ELECTRONIC JOURNAL "PIONEERING STUDIES AND THEORIES"*, *1*(2), 9-13. https://www.pstjournal.uz/index.php/pst/article/view/8

Ayedh M, A. T., Wahab, A. W. A., & Idris, M. Y. I. (2023). Systematic Literature Review on Security Access Control Policies and Techniques Based on Privacy Requirements in a BYOD Environment: State of the Art and Future Directions. *Applied Sciences*, *13*(14), 8048. https://doi.org/10.3390/app13148048

Bada, M., Von Solms, B., & Agrafiotis, I. (2018). Reviewing national cybersecurity awareness in Africa: an empirical study. In *2018* International Conference on CyberTechnologies and Cyber-Systems. https://api.repository.cam.ac.uk/server/api/core/bitstreams/5c149709-b619-4f5d-8f9f-14fdba467e45/content,

Bajwa, U., Gastaldo, D., Di Ruggiero, E., & Knorr, L. (2018). The health of workers in the global gig economy. *Globalization and health*, *14*, 1-4. https://doi.org/10.1186/s12992-018-0444-8

Balozian, P., Leidner, D., & Warkentin, M. (2019). Managers' and employees' differing responses to security approaches. *Journal of Computer Information Systems*, *59*(3), 197-210. https://doi.org/10.1080/08874417.2017.1318687

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. (2018). Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems*, *19*(8), 3. https://doi.org/10.17705/1jais.00506

Barratt, T., Goods, C., & Veen, A. (2020). 'I'm my own boss…': Active intermediation and 'entrepreneurial'worker agency in the Australian gig-economy. *Environment and Planning A: Economy and Space*, *52*(8), 1643-1661. https://doi.org/10.1177/0308518X20914346

Bay, M. (2016). What is cybersecurity. *French Journal for Media Research*, *6*, 1-28. https://frenchjournalformediaresearch.com/lodel-1.0/main/docannexe/file/988/morten_pdf.pdf
Beyond Identity. (2023). *Companies' Cybersecurity Concerns With Gig Economy*. Beyond Identity. Retrieved 25 February 2023 from https://www.beyondidentity.com/cybersecurity-concerns-with-gig-economy
Bhattacherjee, A. (2012). *Social science research: Principles, methods, and practices*. https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1002&context=oa_textbooks
Bowen, G. A. (2006). Grounded theory and sensitizing concepts. *International journal of qualitative methods*, *5*(3), 12-23. https://doi.org/10.1177/160940690600500304
Braun, V., Clarke, V., Boulton, E., Davey, L., & McEvoy, C. (2021). The online survey as a qualitative research tool. *International journal of social research methodology*, *24*(6), 641-654. https://doi.org/10.1080/13645579.2020.1805550
Broughton, A., Gloster, R., Marvell, R., Green, M., & Martin, A. (2018). *The experiences of individuals in the gig economy*. https://www.gov.uk/government/publications/gig-economy-research
Butler, K. J., & Brown, I. (2023). COVID-19 pandemic-induced organisational cultural shifts and employee information security compliance behaviour: a South African case study. *Information & Computer Security*, *31*(2), 221-243. https://doi.org/10.1108/ICS-09-2022-0152
Cant, C. (2019). *Riding for Deliveroo: resistance in the new economy*. John Wiley & Sons.
Casula, M., Rangarajan, N., & Shields, P. (2021). The potential of working hypotheses for deductive exploratory research. *Quality & Quantity*, *55*(5), 1703-1725. https://doi.org/10.1007/s11135-020-01072-9
Chakkaravarthy, S. S., Sangeetha, D., & Vaidehi, V. (2019). A survey on malware analysis and mitigation techniques. *Computer Science Review*, *32*, 1-23. https://doi.org/10.1016/j.cosrev.2019.01.002
Chaudhary, H., Detroja, A., Prajapati, P., & Shah, P. (2020). A review of various challenges in cybersecurity using artificial intelligence. In *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, (pp. 829-836), IEEE, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9316003,
Chen, H., Li, Y., Chen, L., & Yin, J. (2021). Understanding employees' adoption of the Bring-Your-Own-Device (BYOD): the roles of information security-related conflict and fatigue. *Journal of Enterprise Information Management*, *34*(3), 770-792. https://doi.org/10.1108/JEIM-10-2019-0318
Chibanda, R., Tsibolane, P., & Nkohla-Ramunenyiwa, T. (2022). Gendered inequality on digital labour platforms in the global south: Towards a freedom-based inclusion. International Conference on Social Implications of Computers in Developing Countries,
Chowdhury, R. (2023). Impact of perceived convenience, service quality and security on consumers' behavioural intention towards online food delivery services: the role of attitude as mediator. *SN Business & Economics*, *3*(1), 29. https://doi.org/10.1007/s43546-023-00422-7
Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13-21. https://doi.org/10.22215/timreview835
Cunliffe, A. L. (2011). Crafting qualitative research: Morgan and Smircich 30 years on. *Organizational research methods*, *14*(4), 647-673. https://doi.org/10.1177/1094428110373658
Da Veiga, A. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. 2016 SAI computing conference (SAI),
Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & security*, *92*, 101713. https://doi.org/10.1016/j.cose.2020.101713
Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: a comprehensive survey. *The Journal of Defense Modeling and Simulation*, *19*(1), 57-106. https://doi.org/10.1177/1548512920951275
Datta, N., Rong, C., Singh, S., Stinshoff, C., Iacob, N., Nigatu, N. S., Nxumalo, M., & Klimaviciute, L. (2023). *Working Without Borders: The Promise and Peril of Online Gig Work*. https://openknowledge.worldbank.org/handle/10986/40066

De Silva, B. (2023). Exploring the Relationship Between Cybersecurity Culture and Cyber-Crime Prevention: A Systematic Review. *International Journal of Information Security and Cybercrime (IJISC)*, *12*(1), 23-29. https://doi.org/10.19107/ijisc.2023.01.03

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human factors in phishing attacks: a systematic literature review. *ACM Computing Surveys (CSUR)*, *54*(8), 1-35. https://doi.org/10.1145/3469886

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & security*, *92*, 101747. https://doi.org/10.1016/j.cose.2020.101747

Dornheim, P., & Zarnekow, R. (2023). Determining cybersecurity culture maturity and deriving verifiable improvement measures. *Information & Computer Security*. https://doi.org/10.1108/ICS-07-2023-0116

Furnell, S., & Shah, J. N. (2020). Home working and cyber security–an outbreak of unpreparedness? *Computer fraud & security*, *2020*(8), 6-12. https://doi.org/10.1016/S1361-3723(20)30084-1

Gartner. (2021). *Contracting for IT Contingent Labor Services*. Gartner. Retrieved 17 February 2023 from https://www.gartner.com/document/4005141?ref=solrAll&refval=355853121

Gartner. (2023). *Top Trends in Cybersecurity 2023*. Gartner. Retrieved 26 April 2023 from https://www.gartner.com/document/4191399?ref=solrAll&refval=364836257

Gcaza, N., & Von Solms, R. (2017a). Cybersecurity culture: an ill-defined problem. Information Security Education for a Global Digital Society: 10th IFIP WG 11.8 World Conference, WISE 10, Rome, Italy, May 29-31, 2017, Proceedings 10, https://doi.org/10.1007/978-3-319-58553-6_9,

Gcaza, N., & Von Solms, R. (2017b). A strategy for a cybersecurity culture: A South African perspective. *The Electronic Journal of Information Systems in Developing Countries*, *80*(1), 1-17. https://doi.org/10.1002/j.1681-4835.2017.tb00590.x

Gcaza, N., Von Solms, R., Grobler, M. M., & Van Vuuren, J. J. (2017). A general morphological analysis: delineating a cyber-security culture. *Information & Computer Security*, *25*(3), 259-278. https://doi.org/doi.org/10.1108/ICS-12-2015-0046

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022a). Detecting insider threat via a cyber-security culture framework. *Journal of Computer Information Systems*, *62*(4), 706-716. https://doi.org/10.1080/08874417.2021.1903367

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022b). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*, *35*(2), 486-505. https://doi.org/10.1057/s41284-021-00286-2

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, *62*(3), 452-462. https://doi.org/10.1080/08874417.2020.1845583

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational research methods*, *16*(1), 15-31. https://doi.org/10.1177/1094428112452151

Gregory, K. (2021). 'My life is more valuable than this': Understanding risk among on-demand food couriers in Edinburgh. *Work, employment and society*, *35*(2), 316-331. https://doi.org/10.1177/0950017020969593

Greitzer, F., Purl, J., Leong, Y. M., & Becker, D. S. (2018). Sofit: Sociotechnical and organizational factors for insider threat. In *2018 IEEE Security and Privacy Workshops (SPW)* (pp. 197-206). IEEE, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8424651,

Herley, C. (2014). Security, cybercrime, and scale. *Communications of the ACM*, *57*(9), 64-71. https://doi.org/10.1145/2654847

Holden, M. T., & Lynch, P. (2004). Choosing the appropriate methodology: Understanding research philosophy. *The marketing review*, *4*(4), 397-409. https://doi.org/10.1061/(asce)0733-9372(1996)122:1(4)

Huang, K., & Pearlson, K. (2019). For what technology can't fix: Building a model of organizational cybersecurity culture. In *52nd Hawaii International Conference on System Sciences, (pp.6398-6407),* https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/7083b12c-3069-42ec-ae0e-0ee6a3989437/content,

Hyde, K. F. (2000). Recognising deductive processes in qualitative research. *Qualitative market research: An international journal*, *3*(2), 82-90. https://doi.org/10.1108/13522750010322089

Ioannou, M., Stavrou, E., & Bada, M. (2019). Cybersecurity culture in computer security incident response teams: Investigating difficulties in communication and coordination. 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security),

Jansen, H. (2010). The logic of qualitative survey research and its position in the field of social research methods. Forum Qualitative Sozialforschung/Forum: Qualitative Social Research, https://www.qualitative-research.net/index.php/fqs/article/view/1450/2947,

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019). Towards an improved understanding of human factors in cybersecurity. *2019 5th International Conference on Collaboration and Internet Computing (CIC),* (*pp. 338-345*) https://ieeexplore-ieee-org.ezproxy.uct.ac.za/document/8998491,

Kabanda, G. (2018). A Cybersecurity culture framework and its impact on Zimbabwean organizations. *Asian Journal of Management, Engineering & Computer Science*, *3*(4), 17-34. https://doi.org/https://www.academia.edu/download/60361766/Gabriel_Paper_AJMECS_Cybersecurity_Culture_Framework20190822-109031-t3ubm9.pdf

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 269-282.

Kaine, S., & Josserand, E. (2019). The organisation and experience of work in the gig economy. *Journal of Industrial Relations*, *61*(4), 479-501. https://doi.org/10.1177/0022185619865480

Kamais, C. E. (2019). Emerging security risks of e-hail transport services: Focus on Uber taxi in Nairobi, Kenya. *International Journal of Security, Privacy and Trust Management (IJSPTM) Vol*, *8*(3), 1-18. https://ssrn.com/abstract=3486764

Kangapi, T. M., & Chindenga, E. (2022). Towards a Cybersecurity Culture Framework for Mobile Banking in South Africa. 2022 IST-Africa Conference (IST-Africa),

Karjalainen, M., Siponen, M., & Sarker, S. (2020). Toward a stage theory of the development of employees' information security behavior. *Computers & security*, *93*, 101782. https://doi.org/10.1016/j.cose.2020.101782

Karlsson, M., Karlsson, F., Åström, J., & Denk, T. (2022). The effect of perceived organizational culture on employees' information security compliance. *Information & Computer Security*, *30*(3), 382-401. https://doi.org/10.1108/ICS-06-2021-0073

Kavesa, K., & Mbali, A. (2022). The Gig Economy, Digital Labour Platforms, and Independent Employment in the Eastern Cape. In: Eastern Cape Socio-economic Consultative Council (ECSECC)). https://ecsecc ….

Keshvadi, S. (2023). Enhancing Western Organizational Cybersecurity Resilience through Tailored Education for Non-Technical Employees. 2023 IEEE International Humanitarian Technology Conference (IHTC),

Kim, Y. G., Chung, Y. K., & Woo, E. (2023). Gig Workers' Quality of Life (QoL) and Psychological Well-Being in Service Delivery Platform. *Sustainability*, *15*(11), 8679. https://doi.org/10.3390/su15118679

Kinder, E., Jarrahi, M. H., & Sutherland, W. (2019). Gig platforms, tensions, alliances and ecosystems: An actor-network perspective. *Proceedings of the ACM on Human-Computer Interaction*, *3*(CSCW), 1-26. https://doi.org/10.1145/3359314

Kioskli, K., Fotis, T., Nifakos, S., & Mouratidis, H. (2023). The importance of conceptualising the human-centric approach in maintaining and promoting cybersecurity-hygiene in healthcare 4.0. *Applied Sciences*, *13*(6), 3410. https://doi.org/10.3390/app13063410

Kravchenko, O., Veklych, V., Krykhivskyi, M., & Madryha, T. (2024). Cybersecurity in the face of information warfare and cyberattacks. *Multidisciplinary Science Journal*, *6*. https://doi.org/10.31893/multiscience.2024ss0219

Kuhn, K. M., Meijerink, J., & Keegan, A. (2021). Human resource management and the gig economy: Challenges and opportunities at the intersection between organizational HR decision-makers and digital labor platforms. *Research in personnel and human resources management*, *39*, 1-46. https://doi.org/10.1108/S0742-730120210000039001

Lee, M. K., Kusbit, D., Metsky, E., & Dabbish, L. (2015). Working with machines: The impact of algorithmic and data-driven management on human workers. *2015 33rd Annual Conference on human factors in computing systems, Crossings, Seoul, Korea, (pp. 1603-1612),* https://doi.org/10.1145/2702123.2702548,

Leech, N. L., & Onwuegbuzie, A. J. (2011). Beyond constant comparison qualitative data analysis: Using NVivo. *School Psychology Quarterly*, *26*(1), 70-84. https://doi.org/10.1037/a0022711

Leenen, L., & van Vuuren, J. J. (2019). Framework for the cultivation of a military cybersecurity culture. Proceedings of the 14th International Conference on Cyber Warfare and Security (ICCWS 2019), Stellenbosch, South Africa,

Lesala Khethisa, B., Tsibolane, P., & Van Belle, J.-P. (2020). Surviving the Gig economy in the global south: How Cape Town domestic workers cope. The Future of Digital Work: The Challenge of Inequality: IFIP WG 8.2, 9.1, 9.4 Joint Working Conference, IFIPJWC 2020, Hyderabad, India, December 10–11, 2020, Proceedings,

Li, J.-h. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1462-1474. https://doi.org/10.1631/FITEE.1800573

Liang, C., Peng, J., Hong, Y., & Gu, B. (2022). The hidden costs and benefits of monitoring in the gig economy. *Information Systems Research*, *34*(1), 297-318. https://doi.org/10.1287/isre.2022.1130

Malik, R., Visvizi, A., & Skrzek-Lubasińska, M. (2021). The gig economy: Current issues, the debate, and the new avenues of research. *Sustainability*, *13*(9), 5023. https://doi.org/10.3390/su13095023

Marotta, A., & Pearlson, K. (2019). A culture of cybersecurity at Banca Popolare di Sondrio. 25th Americas Conference on Information Systems, AMCIS, Cancun, Mexico, March 1, 2019, Proceedings (pp 1- 10). https://cams.mit.edu/wp-content/uploads/BPS-Case-Study-03012019.pdf,

Masombuka, M., Grobler, M., & Watson, B. (2018). Towards an artificial intelligence framework to actively defend cyberspace. *European Conference on Information Warfare and Security, ECCWS, June, 2018, (pp. 589 - 596). https://www.proquest.com/docview/2077000322?pq-origsite=gscholar&fromopenview=true*,

Mazzarolo, G., & Jurcut, A. D. (2019). Insider threats in Cyber Security: The enemy within the gates. *arXiv preprint arXiv*. http://arxiv.org/abs/1911.09575

Meyer, D. F. (2021). An assessment of the impact of the tourism sector on regional economic development in gauteng province, South Africa. In C. Rui Alexandre, C. Gualter, & S. Rossana (Eds.), *Peripheral territories, tourism, and regional development* (pp. Ch. 7). IntechOpen. https://doi.org/10.5772/intechopen.95810

Moletsane, T., & Tsibolane, P. (2020). Mobile information security awareness among students in higher education: An exploratory study. 2020 Conference on Information Communications Technology and Society (ICTAS), Durban, South Africa.

Montgomery, T., & Baglioni, S. (2021). Defining the gig economy: platform capitalism and the reinvention of precarious work. *International Journal of Sociology and Social Policy*, *41*(9/10), 1012-1025. https://doi.org/10.1108/IJSSP-08-2020-0400

Mpofu, T., Tsibolane, P., Heeks, R., & Van Belle, J.-P. (2020). Risks and risk-mitigation strategies of gig economy workers in the global South: The case of ride-hailing in Cape Town. International Conference on Social Implications of Computers in Developing Countries,

Mwim, E. N., & Mtsweni, J. (2022). Systematic review of factors that influence the cybersecurity culture. Human Aspects of Information Security and Assurance: 16th IFIP WG 11.12 International Symposium, HAISA 2022, Mytilene, Lesbos, Greece, July 6–8, 2022, Proceedings (pp. 147-172). https://link.springer.com/chapter/10.1007/978-3-031-12172-2_12,

Ncubukezi, T., Mwansa, L., & Rocaries, F. (2020). A review of the current cyber hygiene in small and medium-sized businesses. 2020 15th International Conference for Internet Technology and Secured Transactions (ICITST),

Ndlovu, M. P., & Tsibolane, P. (2025). Exploring Organizational Resilience Towards AI-Driven Cyber Threats: A Systematic Literature Review. IST-Africa 2025

Niu, Z. (2022). *Develop and adopt the organizational cybersecurity culture in the Covid-19 teleworking scenario* University of Twente]. http://essay.utwente.nl/92817/1/NIU_MA_EEMCS.pdf

Onumo, A., Ullah-Awan, I., & Cullen, A. (2021). Assessing the moderating effect of security technologies on employees compliance with cybersecurity control procedures. *ACM Transactions on Management Information Systems (TMIS)*, *12*(2), 1-29. https://doi.org/10.1145/3424282

Pankaj, A. K., & Jha, M. K. (2024). Gig workers in precarious life: The trajectory of exploitation, insecurity, and resistance. *American Journal of Economics and Sociology*. https://doi.org/10.1111/ajes.12563

Pearse, N. (2019). An illustration of deductive analysis in qualitative research. 18th European conference on research methodology for business and management studies, Wits Business School, Johannesburg, South Africa, 20-21, June, 2019. http://eprints.lincoln.ac.uk/id/eprint/36421/1/ECRM19-Proceedings-Download.pdf#page=279,

Peterson, C. L., & Steinbaum, M. (2023). Coercive rideshare practices: At the intersection of antitrust and consumer protection law in the gig economy. *University of Chicago Law Review*, *90*(2), 623-658. https://heinonline.org/HOL/Print?collection=journals&handle=hein.journals/uclr90&id=636

Ponelis, S. R. (2015). Using interpretive qualitative case studies for exploratory research in doctoral studies: A case of information systems research in small and medium enterprises. *International Journal of Doctoral Studies*, *10*, 535. https://doi.org/10.28945/2339

Puram, P., Gurumurthy, A., Narmetta, M., & Mor, R. S. (2021). Last-mile challenges in on-demand food delivery during COVID-19: understanding the riders' perspective using a grounded theory approach. *The International Journal of Logistics Management*, *33*(3), 901-925. https://doi.org/10.1108/IJLM-01-2021-0024

Raeff, C., Fasoli, A. D., Reddy, V., & Mascolo, M. F. (2020). The concept of culture: Introduction to spotlight series on conceptualizing culture. *24*(4), 295-298. https://doi.org/10.1080/10888691.2020.1789344

Ratchford, M., El-Gayar, O., Noteboom, C., & Wang, Y. (2022). BYOD security issues: A systematic literature review. *Information Security Journal: A Global Perspective*, *31*(3), 253-273. https://doi.org/10.1080/19393555.2021.1923873

Reid, R., & Van Niekerk, J. (2014). From information security to cyber security cultures. 2014 Information Security for South Africa, Johannesburg, South Africa, August, 2014, pp. 1-7, https://10.1109/ISSA.2014.6950492.,

Rohan, R., Funilkul, S., Pal, D., & Chutimaskul, W. (2021). Understanding of human factors in cybersecurity: A systematic literature review. 2021 International Conference on Computational Performance Evaluation (ComPE), North-Eastern Hill University, Shillong, Meghalaya, India. Dec 1-3, 2021, https://10.1109/ComPE53109.2021.9752358,

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students*. Harlow: Pearson Education Limited.

Schein, E. H. (2004). *Organizational culture and leadership* (Vol. 3). John Wiley & Sons.

Senyo, P., Karanasios, S., Agbloyor, E. K., & Choudrie, J. (2024). Government-Led digital transformation in FinTech ecosystems. *The Journal of Strategic Information Systems*, *33*(3), 101849. https://doi.org/10.1016/j.jsis.2024.101849

Shan, Z., & Yao, J. (2024). Resource Scheduling Optimization of Fresh Food Delivery Porters Considering Ambient Temperature Variations. *Sustainability*, *16*(9), 3624. https://doi.org/10.3390/su16093624

Shankar, A., Jebarajakirthy, C., Nayal, P., Maseeh, H. I., Kumar, A., & Sivapalan, A. (2022). Online food delivery: A systematic synthesis of literature and a framework development. *International Journal of Hospitality Management*, *104*, 103240. https://doi.org/10.1016/j.ijhm.2022.103240

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & security*, *119*, 102756. https://doi.org/10.1016/j.cose.2022.102756

SNS Insider. (2023). *BYOD Security Market Size, Share, Growth & Trend Report 2023*. Retrieved 13 June 2024 from https://www.researchgate.net/publication/371946001_BYOD_Security_Market_Size_Share_Growth_Trend_Report_2023

Society for Industrial and Organizational Psychology. (2023). *Top 10 Work Trends*. Retrieved 09 April 2023 from https://www.siop.org/Business-Resources/Top-10-Work-Trends

Solomon, G., & Brown, I. (2021). The influence of organisational culture and information security culture on employee compliance behaviour. *Journal of Enterprise Information Management*, *34*(4), 1203-1228. https://doi.org/10.1108/JEIM-08-2019-0217

Splunk. (2024). *State of Security, The Race to Harness AI*. https://www.splunk.com/en_us/form/state-of-security/thanks.html

Statistics South Africa. (2023). *Quarterly Labour Force Survey (QLFS) Q1:2023*. https://www.statssa.gov.za/publications/P0211/Presentation%20QLFS%20Q1%202023.pdf

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research* (Vol. 1). Sage

Subashini, P., Krishnaveni, M., Dhivyaprabha, T., & Shanmugavalli, R. (2020). Review on intelligent algorithms for cyber security. *Handbook of Research on Machine and Deep Learning Applications for Cyber Security*(February), 1-22. https://doi.org/10.4018/978-1-5225-9611-0.ch001

Sun, P. (2019). Your order, their labor: An exploration of algorithms and laboring on food delivery platforms in China. *Chinese Journal of Communication*, *12*(3), 308-323. https://doi.org/10.1080/17544750.2019.1583676

Surfshark. (2022). *Cybercrime Statistics*. Retrieved 23 June 2023 from https://surfshark.com/research/data-breach-impact/statistics

Suri, H. (2011). Purposeful sampling in qualitative research synthesis. *Qualitative research journal*, *11*(2), 63-75. https://doi.org/10.3316/QRJ1102063

Sutton, A., & Tompson, L. (2024). Towards a Cybersecurity Culture-Behaviour Framework: A Rapid Evidence Review. *Computers & security*, 104110. https://doi.org/10.1016/j.cose.2024.104110

Swedberg, R. (2020). Exploratory research. In *The production of knowledge: Enhancing progress in social science* (pp. 17-41). https://doi.org/10.1017/9781108762519.002

Tan, Z. M., Aggarwal, N., Cowls, J., Morley, J., Taddeo, M., & Floridi, L. (2021). The ethical debate about the gig economy: A review and critical analysis. *Technology in Society*, *65*, 101594. https://doi.org/10.1016/j.techsoc.2021.101594

Thomas, S. M., & Baddipudi, V. (2022). Changing nature of work and employment in the gig economy: The role of culture building and leadership in sustaining commitment and job satisfaction. *NHRD Network Journal*, *15*(1), 100-113. https://doi.org/10.1177/26314541211064735

TimesLive. (2023). *Gauteng government partners with UberEats to 'unlock e-commerce opportunities for township business'*. Retrieved 08 August 2023 from https://www.timeslive.co.za/news/south-africa/2023-08-03-gauteng-government-partners-with-ubereats-to-unlock-e-commerce-opportunities-for-township-business/

Torres, C. I., & Crossler, R. E. (2024). Promoting security behaviors in remote work environments: Personal values shaping information security policy compliance. *Information Systems Research*. https://doi.org/10.1287/isre.2021.0563

Turner, C., & Astin, F. (2021). Grounded theory: what makes a grounded theory study? *European Journal of Cardiovascular Nursing*, *20*(3), 285-289. https://doi.org/10.1093/eurjcn/zvaa034

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & security*, *109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

Ungureanu, A. (2019). Industry 4.0. The role of gig economy in the industrial revolution of the 21st century. *The USV Annals of Economics and Public Administration*, *19*(2 (30)), 77-84. http://annals.seap.usv.ro/index.php/annals/article/viewArticle/1162

Urquhart, C. (2012). *Grounded theory for qualitative research: A practical guide*. SAGE Publications Ltd.

Vallas, S., & Schor, J. B. (2020). What do platforms do? Understanding the gig economy. *Annual Review of Sociology*, *46*, 273-294. https://doi.org/10.1146/annurev-soc-121919-054857

Van Belle, J.-P., Howson, K., Graham, M., Heeks, R., Bezuidenhout, L., Tsibolane, P., du Toit, D., Fredman, S., & Mungai, P. (2023). Fair work in South Africa's gig economy: A journey of engaged scholarship. *Digital Geography and Society*, *5*(June 2023), 100064. https://doi.org/10.1016/j.diggeo.2023.100064

Van Der Kleij, R. (2022). From Security-as-a-Hindrance Towards User-Centred Cybersecurity Design. *Hum. Factors Cybersecur*, *53*, 120-127. https://doi.org/10.54941/ahfe1002209

Veen, A., Barratt, T., & Goods, C. (2020). Platform-capital's 'app-etite'for control: A labour process analysis of food-delivery work in Australia. *Work, Employment and Society*, *34*(3), 388-406. https://doi.org/10.1177/0950017019836911

Verizon. (2022). *Data Breach Investigations Report*. Retrieved 07 March 2023 from https://www.verizon.com/business/resources/Tc2e/reports/dbir/2022-data-breach-investigations-report-dbir.pdf

Vignola, E. F., Baron, S., Abreu Plasencia, E., Hussein, M., & Cohen, N. (2023). Workers' Health under Algorithmic Management: Emerging Findings and Urgent Research Questions. *International Journal of Environmental Research and Public Health*, *20*(2), 1239.

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, *128*, 113160. https://doi.org/10.1016/j.dss.2019.113160

Wang, S., Li, L. Z., & Coutts, A. (2022). National survey of mental health and life satisfaction of gig workers: the role of loneliness and financial precarity. *BMJ open*, *12*(12), e066389. https://doi.org/10.1136/bmjopen-2022-066389

Warrington, C., Syed, J., & Tappin, R. M. (2021). Personality and employees' information security behavior among generational cohorts. *Computer and Information Science*, *14*(1), 1-44. https://doi.org/10.5539/cis.v14n1p44

Watson, G. P., Kistler, L. D., Graham, B. A., & Sinclair, R. R. (2021). Looking at the gig picture: Defining gig work and explaining profile differences in gig workers' job demands and resources. *Group & Organization Management*, *46*(2), 327-361. https://doi.org/10.1177/1059601121996548

Wiener, N. (2019). *Wiener, Norbert. Cybernetics or Control and Communication in the Animal and the Machine*.

Williams, M., & Moser, T. (2019). The art of coding and thematic exploration in qualitative research. *International management review*, *15*(1), 45-55.

Willie, M. M. (2023). The role of organizational culture in cybersecurity: Building a security-first culture. *Journal of Research, Innovation and Technologies*, *2*(2 (4)), 179-198. https://doi.org/10.57017/jorit.v2.2(4).05

Wood, A. J. (2021a). Algorithmic management consequences for work organisation and working conditions. *JRC Working Papers Series on Labour, Education and Technology*, *2021*(07).

Wood, A. J. (2021b). Algorithmic management consequences for work organisation and working conditions. https://doi.org/https://ec.europa.eu/jrc

Wood, A. J., Graham, M., Lehdonvirta, V., & Hjorth, I. (2019). Good gig, bad gig: autonomy and algorithmic control in the global gig economy. *Work, employment and society*, *33*(1), 56-75. https://doi.org/10.1177/0950017018785616

Woodcock, J., & Graham, M. (2019). *The gig economy. A critical introduction.* Cambridge: Polity.

World Economic Forum. (2024). *Global Cybersecurity Outlook 2024*. Retrieved 15 April 2024 from https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

Zaidi, S. B. (2022). Situating sensitizing concepts in the constructivist-critical grounded theory method. *International journal of qualitative methods*, *21*, 1-13. https://doi.org/10.1177/16094069211061957

# 8 Appendixes

## Appendix A - Semi-Structured Interview Questions

| | |
|---|---|
| **General Questions** | |
| • **Introduce myself and give background about the study.**<br>• **Welcome participant and give them additional information about informed consent and how the data will be used.**<br>• **Give participant breakdown on the interview.**<br>• **Inform participant that interview will be 30 to 60 mins.** | |
| 1 | How long have you worked as a gig worker? |
| 2 | Which companies have you worked for? |
| 3 | What is your highest level of education? |
| 4 | Are you familiar with the following term cybersecurity? |
| **External Influences** | |
| 5 | 5.1 How do you perceive the organisation's awareness of external cybersecurity influences, such as industry regulations, emerging threats, and best practices?<br><br>5.2 Does the organisation regularly send you updates on the latest threats that may impact similar organisations as yours?<br><br>5.3 Do you as gig workers have discussions among yourselves regarding cybersecurity? |
| **Management Mechanisms** | |
| 6 | **<u>Management Support</u>**<br><br>6.1 As a gig worker, has management engaged you on specific cybersecurity initiatives?<br><br>6.2 Have you observed any interaction from management regarding cybersecurity and how does this influence the overall cybersecurity culture within the organisation? |
| 7 | **<u>Policies and Procedures</u>**<br><br>7.1 As a gig worker, how familiar are you with the organisation's cybersecurity policies and procedures?<br><br>7.2 How often are policies and procedures communicated to you? |

| | |
|---|---|
| | 7.3 Have you encountered instances where these policies directly influence your work, and how effectively have they been communicated to you? |
| 8 | **Security Education Awareness and Training**<br><br>8.1 In your role as a gig worker, have you participated in any security education, awareness, or training?<br><br>8.2 Has the organisation facilitated any sort of training for you?<br><br>8.3 How would you say you keep up to date with the latest cybersecurity trends? |
| **Psychological Factors** | |
| 9 | **Beliefs**<br><br>9.1 As a gig worker do your beliefs regarding cybersecurity align with the beliefs that are promoted by the organisation?<br><br>9.2 During your time as a gig worker and interaction with other gig workers, what would you say motivates you and fellow gig workers to report security incidents? Is there a portal to report it? |
| 10 | **Values**<br><br>10.1 As a gig worker, can you describe any core values that the organisation appears to prioritise in relation to cybersecurity?<br><br>10.2 Does the organisation display these values?<br><br>10.3 During your time as a gig worker, have you identified any specific values that fellow gig workers seem to uphold when it comes to incorporating cybersecurity considerations into their work?<br><br>10.4 Would you say values play a role in driving cybersecurity behaviour? |
| 11 | **Attitudes**<br><br>11.1 In your time as a gig worker, what attitudes towards cybersecurity have you observed among your fellow gig workers?<br><br>11.2 Would you say positive attitudes drive employees to seek knowledge and stay informed about cybersecurity? |

**Appendix A.1 - Semi-Structured Interview Questions - Refined**

| **General Questions** |
|---|
| • **Introduce myself and give background about the study.**<br><br>The study aims to understand how cybersecurity culture influences food delivery gig workers' cybersecurity behaviour. Furthermore, the study aims to understand and describe the cultural factors influencing the cybersecurity behaviour of food delivery gig workers. There are two research questions that the study aims to answer:<br><br>1. How does the cybersecurity culture influence the cybersecurity behaviours of food delivery gig workers?<br><br>2. What factors influence cybersecurity culture among food delivery gig workers?<br><br>The study is significant because it contributes to the Information Systems body of work, particularly cybersecurity behavioural factors amongst food-delivery gig economy workers in Gauteng, South Africa.<br><br>• **Welcome participant and give them additional information about informed consent and how the data will be used.**<br>• **Give participant breakdown of the interview.**<br>• **Inform participant that the interview will be 30 to 60 mins.**<br>• **Inform participants that the interview will be recorded, and that the data will be stored securely.**<br>• **Explain concepts to the participants.**<br>• **Commence with the interview.** |

| **General Questions** | |
|---|---|
| 1.1 | How old are you? |
| 1.2 | Which gender do you identify with? (Opt-Out) |
| 1.3 | Where are you from? What is your nationality?<br><br>(Collecting information about the cultural background of gig workers to understand how cultural norms impact cybersecurity behaviours.) |
| 1.4 | What is your highest level of education? |
| 1.5 | How long have you worked as a food delivery worker? |
| 1.6 | Which companies have you worked for? |
| 1.7 | How would you describe your language proficiency?<br><br>(Assessing language proficiency can help tailor awareness programs to ensure effectiveness) |

| | |
|---|---|
| 1.8 | How would you describe your technical expertise, particularly with the apps and tools required for your work?<br><br>(proficiency in using digital tools and platforms, can provide insights into their comfort level with technology and cybersecurity practices). |
| 1.9 | What is your familiarity with the concept of cybersecurity? How do you apply it in your daily work?<br><br>Explain Cybersecurity. |
| **Cybersecurity Culture Initiatives Implementation Challenges** | |
| 2 | 2.1 How familiar are you with the cybersecurity policies of the platform(s) you work for?<br><br>2.2 Can you share an example of a situation where a cybersecurity policy directly impacted your work?<br><br>2.3 How are cybersecurity policies and updates communicated to you?<br><br>2.4 Have you received any cybersecurity training or education from the platform(s) you work for?<br><br>2.5 What training have you received from the platform (s) you have worked for?<br><br>2.5 How do you keep yourself informed about cybersecurity threats and best practices?<br><br>2.6 How would you describe management's involvement in promoting cybersecurity initiatives?<br><br>2.7 Can you identify any support or challenges from management regarding cybersecurity-related issues? |
| **Dimension 2: Food-Delivery Worker Centric Needs and Preferences** | |
| 3 | 3.1 What are your primary concerns regarding personal safety and security while performing delivery tasks? Do you think cybersecurity plays any role in personal safety?<br><br>3.2 Do you think the platform(s) you work for consider your safety when designing cybersecurity measures?<br><br>3.3 How do you think cybersecurity policies or practices affect the flexibility that food delivery work offers?<br><br>3.4 Have you encountered any conflicts between maintaining cybersecurity and your need for flexibility in food-delivery work? |

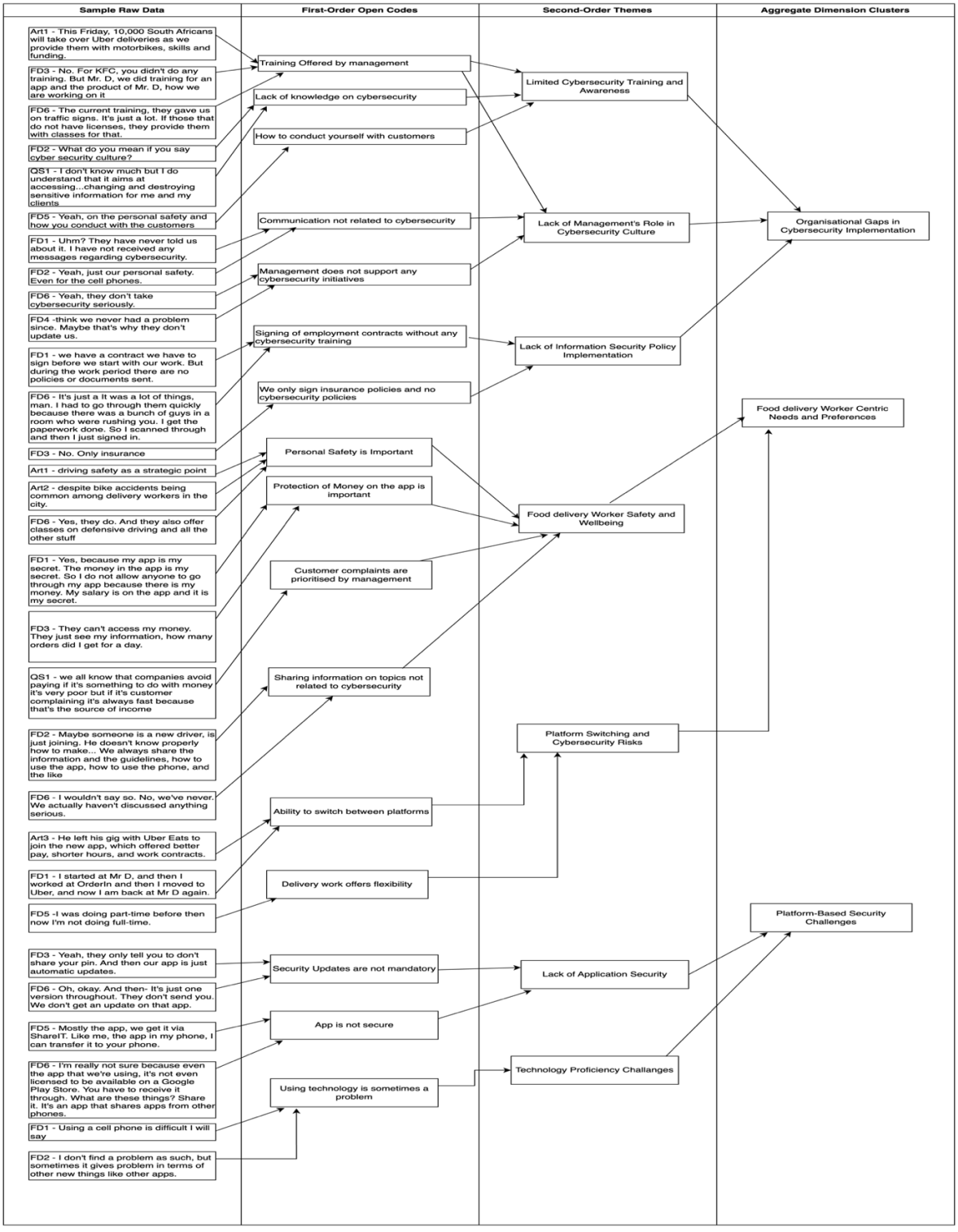
| | |
|---|---|
| **Dimension 3: Platform-Based Security Challenges** | |
| 4 | 4.1 How often do you receive updates about security features on the platforms you use?<br><br>4.2 Do you feel that these updates are necessary or helpful in your work?<br><br>4.3 Have you ever experienced or noticed vulnerabilities in apps you use? How did you respond? How did you initially receive the app when you started?<br><br>4.4 How confident are you in the security of the apps you use for work?<br><br>4.5 How would you rate your comfort with using technology, especially the apps and tools required for food-delivery?<br><br>4.6 What kind of support do you think would help improve your use of technology and understanding of cybersecurity? |
| **Psychological Factors** | |
| 6 | **Beliefs**<br><br>6.1 As a food delivery worker do your beliefs regarding cybersecurity align with the beliefs that are promoted by the organisation?<br><br>6.2 What motivates you to follow cybersecurity guidelines, if any, provided by the platform?<br><br>6.3 Have you experienced any cybersecurity incidents? How was it handled? |
| 7 | **Values**<br><br>7.1 As a food delivery worker, can you describe any core values that the organisation appears to prioritise in relation to cybersecurity?<br><br>7.2 Does the organisation display these values?<br><br>7.3 How do your personal values influence your approach to cybersecurity in your work? |
| 8 | **Attitudes**<br><br>8.1 In your time as a food delivery worker, what attitudes towards cybersecurity have you observed among your fellow food delivery workers?<br><br>8.2 Would you say positive attitudes drive employees to seek knowledge and stay informed about cybersecurity?<br><br>8.3 How important do you think cybersecurity is to the success of your delivery tasks? |

## Appendix B - Qualitative Research Survey Questions

| | |
|---|---|
| **General Questions** | |
| 1 | How long have you worked as a gig worker? |
| 2 | Which companies have you worked for? |
| 3 | What is your highest level of education? |
| 4 | Are you familiar with the following term cybersecurity? |
| **External Influences** | |
| 5 | 5.1 How do you perceive the organisation's awareness of external cybersecurity influences, such as industry regulations, emerging threats, and best practices?<br><br>5.2 Does the organisation regularly send you updates on the latest threats that may impact similar organisations as yours?<br><br>5.3 Do you as gig workers have discussions among yourselves regarding cybersecurity? |
| **Management Mechanisms** | |
| 6 | **Management Support**<br><br>6.1 As a gig worker, has management engaged you on specific cybersecurity initiatives?<br><br>6.2 Have you observed any interaction from management regarding cybersecurity and how does this influence the overall cybersecurity culture within the organisation? |
| 7 | **Policies and Procedures**<br><br>7.1 As a gig worker, how familiar are you with the organisation's cybersecurity policies and procedures?<br><br>7.2 How often are policies and procedures communicated to you?<br><br>7.3 Have you encountered instances where these policies directly influence your work, and how effectively have they been communicated to you? |
| 8 | **Security Education Awareness and Training**<br><br>8.1 In your role as a gig worker, have you participated in any security education, awareness, or training? |

| | |
|---|---|
| | 8.2 Has the organisation facilitated any sort of training for you?<br><br>8.3 How would you say you keep up to date with the latest cybersecurity trends? |
| **Psychological Factors** | |
| 9 | **Beliefs**<br><br>9.1 As a gig worker do your beliefs regarding cybersecurity align with the beliefs that are promoted by the organisation?<br><br>9.2 During your time as a gig worker and interaction with other gig workers, what would you say motivates you and fellow gig workers to report security incidents? Is there a portal to report it? |
| 10 | **Values**<br><br>10.1 As a gig worker, can you describe any core values that the organisation appears to prioritise in relation to cybersecurity?<br><br>10.2 Does the organisation display these values?<br><br>10.3 During your time as a gig worker, have you identified any specific values that fellow gig workers seem to uphold when it comes to incorporating cybersecurity considerations into their work?<br><br>10.4 Would you say values play a role in driving cybersecurity behaviour? |
| 11 | **Attitudes**<br><br>11.1 In your time as a gig worker, what attitudes towards cybersecurity have you observed among your fellow gig workers?<br><br>11.2 Would you say positive attitudes drive employees to seek knowledge and stay informed about cybersecurity? |

# Appendix C – Coding Exercise and Data Structure



## Appendix D – Individual Consent Form

**Department of Information Systems**
Leslie Commerce Building
Engineering Mall, Upper Campus
OR
Private Bag X3 - Rondebosch - 7701
Tel: +27 (0) 21 650 2261 Fax: +27 (0) 21650 2280
Internet: http://www.commerce.uct.ac.za/informationsystems/

08 January 2024

Request to conduct research and interview participation consent form

Dear Sir/Madam,

In terms of the requirements for completing a Masters of Commerce (Mcom) Degree in Information Systems at the University of Cape Town a research study is required. Your participation in this research is voluntary. All information will be treated in a confidential manner and used exclusively for the purpose of this study. No individual names will be recorded or published. You will not be requested to supply any identifiable information, ensuring anonymity of your responses. You can choose to withdraw from the research at any time for whatever reason, in accordance with ethical research requirements.

The researcher, in this case Mlungisi Radebe, has chosen to conduct a case study entitled, *Understanding the role of cybersecurity culture in the gig economy: The case of platform-based food delivery workers in Gauteng*. The research objectives are to understand how cybersecurity culture influences food delivery gig workers' cybersecurity behaviour and to describe the cybersecurity cultural factors that influence food delivery gig workers' cybersecurity behaviour.

The data collection method will be one-on-one interviews with the food-delivery gig workers. The interviews will be conducted through media platforms such as Microsoft Teams, Zoom, Skype and in person where possible, lasting 30 to 45 minutes. The interviews will be recorded. If you are willing to participate in this study, kindly sign the attached form and return it to me at your earliest convenience.

Should you have any questions regarding this research, please get in touch with me on 081 539 7790 or email RDBMLU003@myuct.ac.za.

Your participation in this study would be greatly appreciated but is entirely voluntary.

Sincerely,

| Mlungisi Radebe | Pitso Tsibolane |
|---|---|
| Masters Student<br>Department of Information Systems<br>University of Cape Town<br>Email: RDBMLU003@myuct.ac.za | Research Supervisor<br>Department of Information Systems<br>University of Cape Town<br>Email: pitso.tsibolane@uct.ac.za |

**Research Participant Consent Form**

I, _____, consent to participate in the research on *Understanding the role of cybersecurity culture in the gig economy: The case of platform-based food delivery workers in Gauteng.*

I am aware that participation is voluntary and that I may choose to withdraw from this study at any time.

_____ _____

Signature Date

## Appendix E – Ethical Clearance Approval

UNIVERSITY OF CAPE TOWN
IYUNIVESITHI YASEKAPA · UNIVERSITEIT VAN KAAPSTAD

2024/01/23

COM/00562/2024

RE: Research Ethics Committee Project Approval Letter

Dear Mlungisi Radebe,

Your application for ethics review of your project titled

Examining the role of cybersecurity culture in the gig economy: The case of platform-based food delivery workers in Gauteng

has been reviewed and evaluated by the

Commerce Research Ethics Committee.

You may proceed with your research project titled:

Examining the role of cybersecurity culture in the gig economy: The case of platform-based food delivery workers in Gauteng

Please note that should:

(i) any serious or adverse effects to participants occur and/or,

(ii) aspect(s) of your current project change and/or

(iii) any unforeseen events that might affect continued ethical acceptability of the project occur then you should immediately report this to the approving REC. You may be required to submit an amendment to this application, in order to determine whether the changed aspects increase the ethical risks of your project.

Based on the information supplied your application has been successful and is approved.

Please note the following additional conditions associated with this approval:

(i)

Regards,

Commerce Research Ethics Committee.

## Appendix F – Online Articles

| Website Reference |
| --- |
| https://www.timeslive.co.za/news/south-africa/2023-08-03-gauteng-government-partners-with-ubereats-to-unlock-e-commerce-opportunities-for-township-business/ |
| https://mybroadband.co.za/news/internet/559414-uber-eats-of-townships-a-massive-hit.html |
| https://restofworld.org/2023/life-of-a-gig-worker-south-africa-food-delivery-driver/ |
| https://mg.co.za/news/2024-07-06-the-appetite-for-food-delivery-services-in-townships-is-growing/ |
| https://thecyberexpress.com/jollibee-cyberattack-claim-customers-data/ |
| https://businesstech.co.za/news/business/798996/criminals-targetting-online-food-delivery-boom-in-south-africa/ |
| https://techpoint.africa/2024/10/07/uber-eats-couriers-safety-south-africa/#:~:text=The%20Safety%20feature%20includes%20a,for%20Uber's%20e%2Dhailing%20consumers. |
| https://businesstech.co.za/news/business/792702/hijackers-coming-after-these-two-targets-in-south-africa/ |
| https://www.linkedin.com/pulse/food-delivery-apps-data-privacy-concerns-protecting-your-information/ |
| https://www.linkedin.com/pulse/securing-digital-feast-cybersecurity-food-delivery-industry-flower-7wk0e/ |
| https://www.controlaudits.com/blog/what-are-the-cybersecurity-best-practices-for-digital-food-delivery/#:~:text=Cybersecurity%20is%20not%20just%20a,the%20appetite%20for%20your%20service. |

## Appendix G – Observation Notes

| |
|---|
| Challenging interview as the participant messaged me early for us to start. Also the participant asked to do the interview in isiZulu as their English is not 100%. Nonetheless, the interview has highlighted some sort of training albeit limited to password sharing and the mandetory updates that are required on the app. Details regarding motivation behind protecting the app stem from protecting the money on the app. Protecting customers from criminals. Not sharing the customer details as this will come back to the driver. Very interesting perspectives. The company does not explicitly state that this is cyber related but they do provide training although it is not sufficient and limited to onboarding only. |
| Vey calm person. Does not say much but understands the value of research and why its important. Gave good insight on the importance of the pin. However, cybersecurity seems to be a new a concept to these guys. The companies do not explicitly train them on cyber. |
| Short interview as the guy gave mostly one word answers. However, it is becoming apparent that Mr D only gives guidance on how to use the app. They only provide a refresher once you are in trouble. It also seems like the app notifies the user to update once there is an update and not because they were alerted by Mr D. Cybersecurity is not something these guys are aware of. |
| What an interesting interview. I learnt that indeed Mr D does force the guys to conduct online e-learning. However, these e-;learnings have got nothing to do with cybersecurity or any form of security. Marlven is a nice guy. He was late for the interview and apologised profusely. He does know what cybersecurity is and the imporatnce of protecting his app and the data on the app. I ended up spending an additional hour with him and his fellow drivers at their hang out spot. Just sitting and talking about their lives. He was robbed a few months back and his bike was hijacked. He was not hurt or anything but was beaten up and shaken up. A good interview overall. Smart guy also. |
| Taku talks a lot and is willing to share a lot of information. He also showed me the e-learning they are required to conduct for Mr D. Nothing to do with security, this is an opportunity for the company to educate the drivers on cyber but they are not taking the opportunity. Also management enagegement is only based on personal saftey and the safety of customers, the parcels and the food they deliver. Overall a good interview. |

## Appendix H – Turnitin Report