

# **A Grounded Theory Study on the InfoSec Resilience of Small and Medium Enterprises: A path independent of Tech Titans**

**Early-stage paper**

**Kennedy Njenga**

Department of Applied Information Systems,  
University of Johannesburg,  
South Africa  
[knjenga@uj.ac.za](mailto:knjenga@uj.ac.za)

## **ABSTRACT**

Small and medium-sized enterprises (SMEs) often face unique information security (InfoSec) challenges due to their size, limited resources, lack of market dominance, and mastery of technology to keep their infrastructure secure. The dominance of tech titans in InfoSec can create a dependency that can be costly and risky for SMEs. This qualitative study shows how SMEs can be InfoSec resilient by taking a path independent of tech titan dominance. The study generated a substantive theory grounded in SME practitioners' real-world practices on InfoSec resilience. This was done using the Grounded Theory (GT) method. The hours of in-depth interviews, guided by theoretical sampling, generated transcripts that were analyzed qualitatively. This analysis generated perspectives that formed the basis of a taxonomy of SME InfoSec resilience on challenges unique to these organizations. The *SME InfoSec Resilience* theory was developed from data grounded in practitioner experience showcasing InfoSec resilience on challenges unique to these organizations. The study offers practical insights for effective InfoSec management and optimization for SMEs.

## ***Keywords***

SMEs, Tech Titans, Information Security, Grounded Theory.

## **INTRODUCTION**

Small and medium-sized enterprises (SMEs) are the engines of economic growth. However, their rapid integration of information technology (IT) and growth has uncovered a formidable challenge: the tech titan. The dominance of the tech titan can create a dependency on SMEs, which is costly and risky. In her book, Webb (2019) talks about how tech titans use artificial intelligence (AI) to shape the future of businesses of all sizes. She mentions nine tech titans, extremely large and comprehensive in scope: Google, Amazon, Apple, IBM, Microsoft, and Facebook (USA), and Baidu, Alibaba, and Tencent (China), all leveraging technology innovation and building AI to boost their InfoSec (InfoSec) postures. Webb (2019) cautions that SMEs lack preparedness for AI's influence on InfoSec and may face existential threats as InfoSec challenges become more sophisticated. Tech titans will continue to flourish in the advent of AI amidst the emergent InfoSec challenges. She points to three scenarios most businesses will face as AI grows in use: optimistic, pragmatic, and catastrophic.

The tech titans are and will continue to be optimistic about using AI because they will use AI to prioritize essential protection and risk assessment across four business life cycle stages: reach acquisition, conversion, and retention (Moradi & Dass, 2022). Google, for instance, can deny or limit access to some businesses in the cyber domain, such as Google Maps, while providing unrestricted access to others. Facebook may allow certain pronouncements on its platform to promote one side of an opinion and restrict pronouncements to those holding conflicting opinions. The tech titan's information-based business means they have unlimited access to the web-based economy, with the means and ability to secure and protect this infrastructure in ways that can create a risky or costly dependency on SMEs (Matania & Sommer, 2023).

Baabdullah et al. (2021) point out that SMEs are slowly beginning to fight back from such dependency and forging an independent path that is InfoSec resilient (Drydakis 2022).

One key challenge, however, is that as SMEs slowly begin to forge this path of independence from tech titans and adopt technology such as AI to be InfoSec resilient, they may potentially expose themselves to more InfoSec challenges. Carbonara and Santarelli (2023) consider SMEs' use of AI as either a threat or an opportunity. Though tech titans are also not immune to security risks, they have the means to invest in out-of-reach technologies to protect themselves. Intentionally or not, with this ability, tech titans can dominate InfoSec while stifling SMEs' security potential.

## **Problem Statement**

SMEs continue to face persistent attacks on their information infrastructure because they lack the capacity to implement Industry 4.0 standards (Arroyabe et al., 2024). SMEs face data ownership challenges due to tech titan dominance, and a data breach at a tech titan could expose sensitive information to multiple SMEs dependent on the tech titan. It is, therefore, necessary to take cognizance of the need for SMEs to be InfoSec resilient to the myriad challenges they face.

## **Research Objectives**

The research has three main objectives:

1. To identify the myriad challenges SMEs face regarding the dominance and dependence of tech titans and how SMEs can be InfoSec resilient.
2. Develop a taxonomy of SME InfoSec resilience and, from this taxonomy, formulate a theory using that can explain InfoSec resilience that may assist SMEs to forge a path independent of tech titans.

This study will leverage the grounded theory approach to address the above objectives and formulate the theory. The following section addresses pertinent literature on InfoSec in SMEs and its resilience.

## **LITERATURE REVIEW**

Three competing variations of the grounded theory approach shaped how the literature review was conducted. The classical (or Glaserian) approach to carrying out a literature review points out that literature is used primarily for verifying and comparing findings and should not necessarily be seen as a starting point for a research study mainly conducted *after* data analysis (Glaser & Strauss, 1967). The second variation, the pragmatic (or Strauss-Corbin) approach, considers the literature review as a resource to inform research questions, guide data collection, and refine theoretical concepts (Strauss & Corbin, 1998). This approach sees the literature review as integral to the research process in theory development and allows the review of literature prior to and during the data collection process. Literature can be used for data comparison to enhance sensitivity and confirm or explain results. While the third approach, the constructivist (or Charmazian) (Charmaz, K., 2008; Mccall & Edwards, 2021), sees the literature review as a possible starting point for conceptualizing the research and critically examines underlying assumptions and biases. It does not prescribe where the review should be placed within the research, and this decision is left to the researcher. If the researcher decides to write it early, it should be revisited to critique and confirm that it aligns with the conclusion.

The literature review for this study follows the pragmatic (or Strauss-Corbin) approach, which will help build theory by firstly, understanding the literature that encompasses the context and environments SMEs operate, secondly, by drawing from these insights that have not been fully

examined, consider how to build theory in these new contexts. The contexts and environments and examined in the next section.

## **Context for InfoSec in SMEs**

Scholars acknowledge that InfoSec management for SMEs plays a crucial role in protecting their critical data and assets (Bolek et al., 2016; Telo, 2019). In South Africa, where this study is domiciled, the Small Business Development Agency (SEDA) has recognized SMEs, or small businesses with less than 500 employees, as a critical source of innovation and flexibility. However, a key challenge is that the failure rate of SMEs in South Africa was about 75% (Fatoki & Odeyemi, 2010). From 2013 to 2019, SMEs in South Africa had an increased turnover of 12.3%, which was higher than large businesses, which increased by only 7.0% (StatsSA, 2024).

The importance of InfoSec is crucial. Indeed, InfoSec safeguards SMEs against data leakage, damage, or misuse, ensuring business continuity and maintaining credibility (Bolek et al., 2016). SMEs are particularly vulnerable to cyberattacks because they lack the necessary resources to protect their valuable business data and customer information they often possess (Bada & Nurse, 2019). Many SMEs bypass compliance requirements, which are perceived as either tedious or difficult to understand, considering that it remains an obligation for SMEs to protect the personal information of their customers and employees (Kosseff, 2016).

In context to relevant laws and regulations such as POPIA, compliance is necessary to avoid legal risks and potential fines (Kosseff, 2016) and to sustain small business development and growth (Bandari, 2023). When SMEs become victims of InfoSec attacks and data breaches, this can have a devastating impact that may disrupt business operations, which may lead to financial losses, reputation damage, and, in worst-case scenarios, legal liabilities (Bandari, 2023). According to

Benz and Chatterjee (2020), SMEs cannot effectively respond to the ever-evolving InfoSec threat landscape, and this hampers their ability to initiate effective security strategies and measures.

SMEs are operated mainly by owner-managers who require above-average skills and technology know-how to mitigate against the evolving InfoSec threat landscape. The owner-manager often plays an important role in safeguarding the SME. They are reputed as the first line of defense for any InfoSec attack. They should, therefore, be equipped with security education, training, and awareness (SETA) to effectively identify potential InfoSec risks and take appropriate measures to protect sensitive data (Conteh & Schmick, 2016). Owner-managers require a robust InfoSec management approach that provides protection to the SME and facilitates an environment that supports SME growth (Conteh & Schmick, 2016). SME owner-managers' limited financial resources and budgets often restrict their ability to invest in sophisticated security solutions or hire dedicated cybersecurity teams (Kurpjuhn, 2015).

### **Context of The Tech Titan Dominance and SME Dependence**

Tech Titans are the biggest and largest players in the business, dominating the use of technology. These companies manage InfoSec threats in vastly different ways compared to SMEs. Because of their size and financial muscle, they can employ top-tier InfoSec practitioners and advanced threat detection systems such as AI-powered Security Information and Event Management (SIEM) to collect data. AI-powered SIEM uses machine learning to analyze vast amounts of data and identify any anomaly that could be a potential threat. Systems like User and Entity Behavior Analytics (UEBA) monitor user behavior patterns that feed into Threat Intelligence Feeds (TIFs).

Because tech titans have vast data stores interconnected with complete networks and services, these Titans have what is considered a larger “attack surface,” meaning that cybercriminals have

a large surface to target. In addition, tech titans have the means and ability to collect vast amounts of user data from SMEs and how they operate, raising concerns about SME privacy and how SME data is used or sold. Because tech titans hold immense power and influence on governments, they have the means and ability to make it difficult for governments to regulate them effectively, potentially hindering fair competition at the expense of SMEs. This is shown in Table 1.

<b>InfoSec Aspect</b>	<b>Tech Titans with AI &amp; ML</b>	<b>SMEs</b>
<b>Threat Detection &amp; Analysis</b>	Machine Learning SIEM (Security Information and Event Management)	Basic SIEM or manual log analysis
<b>User Behavior Monitoring</b>	User and Entity Behavior Analytics (UEBA)	Limited user behavior monitoring
<b>Security architecture</b>	zero-trust architecture, “never trust, always verify”	Basic architecture
<b>Remote work</b>	Secure Access Service Edge (SASE): securing remote workforces and branch offices.	None defined
<b>Processes and operations</b>	Security Automation and Orchestration: Automate routine security tasks (vulnerability scanning, log analysis, incident response)	Manual or reactive responses to InfoSec incidents
<b>Blockchain technology for security</b>	Provides distributed secure recording and transaction verification, protecting data integrity and traceability	Basic or non-existent

**Table 1. Tech Titans InfoSec compared to SMEs**

## InfoSec Resilience

The concept of resilience is closely related to the concepts of robustness, agility, and reliability and is considered the ability of a system to return to its original state or move to a new, more desirable state and be disturbed (Christopher & Peck, 2004). Goel et al. (2023) have studied information systems security resilience (ISSR) and argued that ISSR is highly interdependent with supply chain resilience, supply chain processes, and their practices. This can be taken to present

the interdependence of SMEs with both technology and the businesses operating around SMEs, such as tech titans. Goel et al. (2023) postulate that supply chains often require adept information management to support the inter-organizational exchange of information among actors in the global business arena. SMEs, therefore, need information that can foster their InfoSec resilience and benchmark that can counter dominance by tech titans. The following section discusses the methodology used in this research.

## RESEARCH METHODOLOGY

The grounded theory (GT) approach was chosen for this study because it was deemed suitable for developing a theory that would explain the resilience of SMEs against the dominance of tech titans regarding InfoSec challenges. Strauss & Corbin (1998), p.12 notes the following concerning the GT approach:

*'Data collection, analysis, and eventual theory stand in close relationship to one another...the researcher begins with an area of study and allows the theory to emerge from the data...grounded theories, because they are drawn from data, are likely to offer insight, enhance understanding, and provide a meaningful guide to action'.*

This GT approach is a flexible framework that helps construct theories derived directly from data by manipulating and comparing coded data with other coded data and literature (Corbin & Strauss, 2014). Corbin and Strauss (1990) list cannons that characterize the GT approach, such as cannon #7, p. 10, "process must be built in theory." Cannon #9 suggests "verification" becomes integral to the GT approach, which the classical GT approach has generally opposed (Glaser & Strauss, 1967) and was part of the chasm between the two methodologists (Hernandez, 2009).



## Data Collection and Theoretical Sampling

Determining data to be collected involved the researcher deciding on the analytical grounds for the sample to be chosen. This process is called theoretical sampling, which was first advanced by Glaser and Strauss (1967) and outlined four strategies: maximizing or minimizing the differences between groups or concepts in the data, as shown in Table 2.

Options for Theoretical sampling, adopted from Glaser and Strauss (1967)		
Group Differences	<i>Concepts in the Data</i>	
	Similar	Diverse
<b>Minimized</b>	Maximum similarity in data leads to: Verifying usefulness of category; Generating basic properties; Establishing a set of conditions for a degree of category. These can be used for prediction.	Identifying/developing fundamental differences under which category and hypothesis vary
<b>Maximized</b>	Identifying/developing fundamental uniformities of greatest scope	Maximum diversity in data quickly forces: dense developing of properties of categories; integrating of categories and properties; delimiting scope of theory

**Table 2. Tech Titans InfoSec compared to SMEs: Source Adopted from Glaser and Strauss (1967).**

According to Strauss and Corbin (1998), p. 202, theoretical sampling

*‘rather than being predetermined before beginning the research, evolves during the process. It is based on concepts that emerged from analysis and that appear to have relevance to the evolving theory...the aim of theoretical sampling is to maximise*

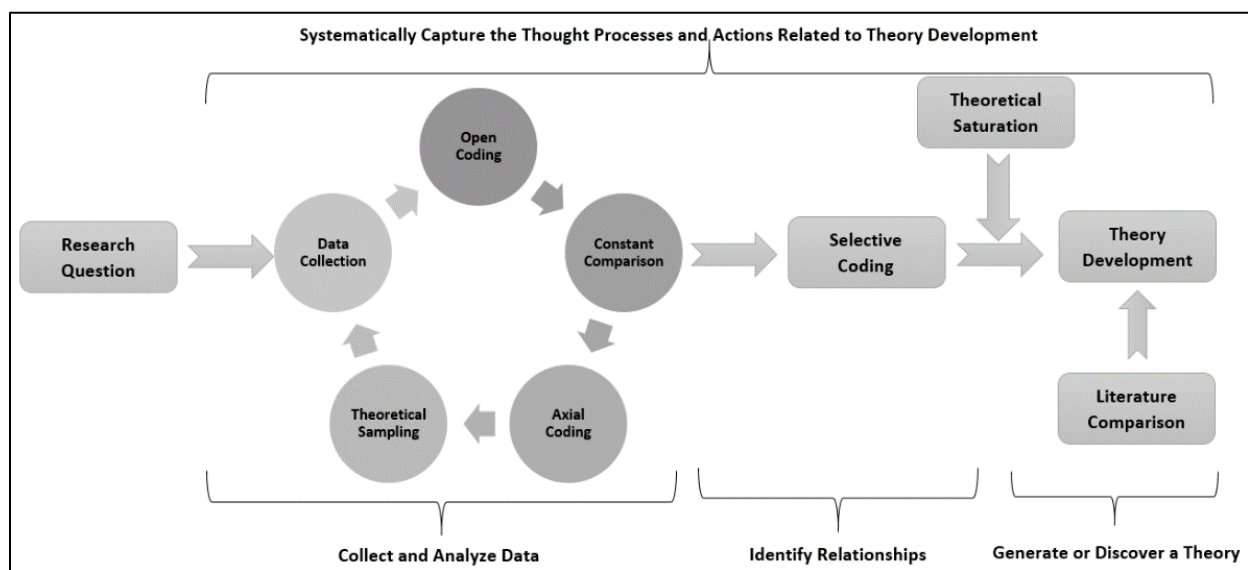
*opportunities to compare events, incidents, or happenings to determine how a category varies in terms of its properties and dimensions’.*

The researcher understood the role of theoretical sampling in planning and getting data from interviews with SME owner-managers because this formed the process of the emergence of theory. Being keen to understand how InfoSec resilient the SME owner-managers were to various challenges, some emanating from tech titans, the researcher did not have predetermined ideas but allowed the SME owner-managers to shape ideas. Therefore, this research started with an initial five participants, who would provide data that would direct the researcher on where to go next. Data elicited from the initial interviews delved into aspects such as the dominance of tech titan technology used by SMEs and the risks this posed. Draucker, Martsolf, and Ross et al. (2007) point out that theoretical sampling will occur when the researcher decides how and where to collect data, how to analyze and code the data, and how to develop a theory from the data. The theoretical sampling used in this study was done to build theory over various data sources such as literature and interviewee transcripts. The researcher looked at the literature and what the five interviewees said and constructed codes, categories, and relationships, looking for patterns and how these patterns might be theorized (Urquhart, 2019). This is to be done until a theory emerges.

## **Coding Data**

This preliminary analysis is called open coding. Coding was done using *Atlas.ti*, a qualitative software used by researchers to analyze qualitative data. Part of the GT method is to seek and identify a sample of practitioners who would best represent the phenomenon of study. The process started with collecting raw data anchored on research questions. The data was recorded and transcribed using AI—the transcribed data generated over 2000 words of qualitative data, providing rich insights into their lived experiences. The transcripts were cleaned (for colloquial

language). Codes were assigned in a process called ‘open coding.’ Urquhart (2000) prescribes how this is to be done: data are broken down, and conceptualization of the meaning is determined. In open codes, meaning is assigned to data, leading to initial concepts. Codes, concepts, and literature are compared in a process called ‘constant comparison’. Selective coding is a process where only relevant concepts are drawn to identify patterns in data. Axial coding looks at these relationships between concepts that have been refined to uncover deeper themes. This process of refinement is done till ‘theoretical saturation.’ These deeper themes form the basis of a substantive theory commonly called ‘grounded theory,’ which is then presented as the final study outcome (Corbin & Strauss, 2014). This process is depicted in Figure 1.



### Figure 1: Grounded Theory method

Source: Corbin & Strauss, (2014).

## Ethics

The researcher obtained permission from the five participants on the condition that their identities were anonymized, and that data would not be individually connected to them. Therefore, the

researcher anonymized all qualitative data used in the study to respect the privacy and confidentiality of participants.

## FINDINGS AND RESULTS

### Sentiment analysis

Sentiment analysis was also carried out using *Atlas.ti*, to obtain an impression of the sentiment held by study participants. This was to provide the researcher with the general sentiment held by study participants in the context of tech titans and InfoSec. The classification of sentiments provided by *Atlas.ti*, were ‘positive,’ ‘neutral,’ and ‘negative’ sentiments. The outcome of sentiment analysis is shown in Table 3.

Sentiment	# of Paragraphs in transcripts	Example sentiments
Positive	2	<i>“There are some ways small businesses can mitigate these existing threats.”</i>
Neutral	49	<i>“Big tech [Tech Titans] often provides educational resources and training on InfoSec best practices.”</i>
Negative	26	<i>“Understandably, I feel frustrated by the lack of control I have over my InfoSec when relying on big tech.” “I sometimes feel apprehensive because I cannot match what these big titans...”</i>

**Table 3. Positive, Neutral, and Negative Sentiment Analysis**

### Concepts and Categories

The study revealed seven main categories derived from the axial coding of 18 concepts. The 18 concepts. These 18 concepts are drawn from open codes depicted in the narrative as code. Codes are underlined for easy identification in transcripts. Hence, analysis moved from many codes to

few concepts to even fewer categories, with the link showing that the substantive theory called the ‘SME Resilience to InfoSec,’ in short, SMER-IS, was derived and grounded from actual raw data. The seven categories were the outcomes of an inductive coding denoting the researcher's interpretation of data. Concepts and categories for this study are shown in Table 4.

	Concepts	Categories	
1	Collaboration	<i>Collaboration and Community</i>	
2	Anger and Frustration	<i>Emotional and Psychological Impact</i>	
3	Anxiety and Concern		
4	Apprehension		
5	Distrust		
6	Overwhelmed		
7	Lack of control		
8	Risk aversion		
9	Adaptability	<i>Adaptability and Innovation</i>	
10	Advancements in technology		
11	Disruption		
12	Vendor Lock-in	<i>Vendor Relations and Dependence</i>	
13	Decision making		
14	Transparency and unfair advantage	<i>Transparency and Fair Practices</i>	
15	Advocacy	<i>Advocacy and Empowerment</i>	
16	Empowerment		
17	Password hygiene	Security and Privacy	
18	Data breach and privacy concerns		

**Table 4. Positive, Neutral, and Negative Sentiment Analysis**

The seven categories are discussed in detail in the sections that follow.

## Collaboration and Community

The category ‘collaboration and community’ emerged from the concept ‘collaboration,’ observed when Participant #2 recognized they lacked capacity and resources like tech titans and the only way was to collaborate. The following transcript echoes this.

*“I pride myself in being forward-thinking. I have viewed partnering with a tech titan like Amazon as a partner in my InfoSec needs. I was looking at the AWS website, and I found that they offer security tools and services such as AWS identity access management and AWS shield. I think that through collaboration, I can protect my data and comply with laws.”*

The above SME sought Amazon Web Services (AWS), a security solution, to address its InfoSec needs. By partnering with AWS, the SME would then focus on its core competencies.

## Emotional and Psychological Impact

The category emotional and psychological impact emerged from seven concepts ‘anger and frustration,’ ‘anxiety and concern,’ ‘apprehension,’ ‘distrust,’ ‘overwhelmed,’ ‘lack of control,’ and ‘risk aversion.’ Participant #4 expressed anger and frustration regarding the potential downsides of collaborating with tech titans. The following transcript echoes this.

*“Understandably, I feel frustrated by the lack of control over my information security when relying on big tech.”*

While Participant #4 considers collaboration necessary, the SME owner felt frustrated about customizing InfoSec measures to their own needs and an apparent power imbalance, which presented an emotional and psychological effect on the SME owner. Similarly, participant #3, echoed the following.

*“You are right, as a small business owner, I am very concerned about information surrounding big tech [tech titans] who can be a major source of worry.”*

Perhaps it was because SMEs were struggling to keep up with the rapid innovation cycle of the tech titans. Nonetheless, this anxiety and concern presented emotional and psychological effects on this SME owner.

It emerged, too, that apprehension was an emotional and psychological trait that SME owners manifested. One SME owner acknowledged resource disparities, and the financial advantage tech titans have. Participant #1 mentioned the following regarding this:

*“I sometimes feel apprehensive because I cannot match what these big titans have in terms of money and cannot afford to pay security professionals. My limited resources make me worry about taking on my small business the additional burden of managing my own security infrastructure. Sometimes, I wait and see, hoping that the tech titans will not be a security concern.”*

While managing their own InfoSec infrastructure can be daunting for SME owners, apprehensiveness can create additional emotional and psychological strain. There is also the fear that the tech titans would be their security threats, exacerbating the emotional strain. Participant #5, a business professional and SME owner questioned tech titans' interests, suspecting that these big businesses only serve their own interests. Participant #5 showed distrust of these businesses by echoing the following:

*“I am sometimes skeptical of big tech's [tech titans] overexaggerated information security claims. I think they want small businesses like us to invest more heavily in*

*their own internal security expertise... they limit our options regarding seeking cheaper independent security solutions.”*

The distrust seemed to emanate from Participant #5 suspicion that tech titans benefit from SMEs focusing heavily on internal security expertise, forcing them to be reliant. The distrust may come from a lack of transparency or external pressure to use tech titans or their affiliates’ InfoSec services. Participant # 3 felt emotionally overwhelmed by the constant barrage of InfoSec threats, feeling that they were constantly and consistently bombarded with new InfoSec threats. The following statement echoes this:

*“You know...I feel that sometimes there is a lot to keep track of! Many times, I keep hearing about this and that security threat...I mean, these new security threats are constantly emerging. What are we to do? Keeping my business secure is difficult, and I feel... it is daunting.”*

Observing that the fast-paced nature of the cybersecurity landscape can be daunting to SME owners, it is hard for these owners to keep up with the latest security best practices. An effort to keep these businesses secure presents a significant emotional and psychological burden on these SME owners. Participant #2 presented the emotion, the feeling of lack of control, which was shown by the following statement:

*“It is understandable to feel frustrated by the lack of control you have over your security when relying on big tech.”*

Observing that when SME owner-managers outsource InfoSec services, inevitably, they also surrender some control over how these services will be implemented and, of importance, how their data will be protected. Indeed, a security breach in a tech titan’s infrastructure could compromise



the security of SME data, presenting an emotional and psychological toll on SME owners. An emotional and psychological trait, risk aversion, was observed when Participant #1 mentioned that:

*“I sometimes adopt a wait-and-see approach. This way, I keep hoping that big tech companies will address information security concerns, and in turn, this will help us...” I do not usually change my [information security] methods.”*

Participant #1 expresses hesitancy and discomfort with changing the existing familiar InfoSec approaches. This owner hopes tech titans will take the lead in addressing InfoSec concerns, potentially minimizing the emotional and psychological burn placed on them to secure their own businesses.

## **Adaptability and Innovation**

The category adaptability and innovation emerged from three concepts, ‘adaptability,’ ‘advancements in technology,’ and ‘disruption.’ SME owners, while acknowledging frustration and even fear in the face of InfoSec threats, seem to respond to threats rather than anticipate these threats, therefore lacking the ability to strategize effectively. Participant #5 highlights the importance of being ready and speedily responding to these InfoSec threats. This is an important and positive aspect of adaptability and agility that can help SMEs adjust to the ever-changing threat environment. Participant #5 mentions the following:

*“Scared? Yes, at times, [I am] frustrated and overwhelmed because of all these security threats, but all said and done, I must adapt and respond to these threats. I will likely have a mix of many reactions, but remember, the more I can respond quickly, the more I will succeed in businesses.”*

Participant #5 mentions “a mix of many emotions,” suggesting that while this owner can be adaptive, they remain uncertain regarding the best course of action. This openness can suggest the potential for the owner to be more proactive and innovative to keep pace with disruptions.

Participant #3 acknowledges limited know-how on the extent to which technology has advanced and states the following:

*“I hear these guys [Tech Titans] can offer small businesses a wealth of affordable security solutions. Someone told me...However, I have not tried it yet, and there are affordable cloud-based firewalls and endpoint protection that [Tech Titans] offer. It would be good for my business to use secure communication across my platforms using these advanced technologies .... Look, on any ordinary day, many of these advanced tools are out of reach for small people.”*

The concept of ‘advancements in technology’ was derived from this statement, with the interpretation that the SME owner may be relying on hearsay and a misconception that these advanced technologies “*are out of reach*.” However, despite this misunderstanding and hesitation, Participant #3 sees potential benefits for technological advances in SME operations, stating that “*it would be good for my business*.”

It was also observed that Participant #4 was fully aware of the potential overreliance on tech titan's InfoSec services, noting the fear of disruption caused by tech titan service outages or of changes in their InfoSec policies. The following statement echoed this.

*“I know that when I become too dependent on Big Tech [tech titan] services for a critical service online, and they experience an outage or even decide to change*

*policy, I will be severely disrupted and scramble for limited options; this is a scary thought, although it has not happened yet.”*

The owner intimates “*scrambling*” for solutions in case of disruption, which suggests that this owner held a reactive rather than proactive disposition to adaptability and innovation in the face of tech titan’s initiatives.

## **Vendor Relations and Dependence**

The category vendor relations and dependence emerged from two concepts: ‘vendor lock-in’ and ‘decision-making.’ A classic case of vendor lock-in was observed from Participant #1, who mentioned the following:

*“I remember this instance where I was locked into a big tech [tech titan] platform. This made me have trouble switching to a cheaper alternative. They seem to make it more expensive to switch , come to think of it...” to another provider...”*

SMEs are typically budget-conscious and will always prioritize any forthcoming InfoSec solution that is cost-effective; this includes switching to new but cheaper solutions that will address their needs. They will dislike any idea that threatens this flexibility. This is why Participant #1 focuses on the need to nurture vendor relations and wean dependency.

At the crux of a well-managed SME are the sound decisions made by the owner. This is particularly important in the face of InfoSec challenges SMEs face. Owners often adopt multiple decision-making roles because of a lack of personnel for InfoSec research and analysis. Participant #3 elaborates as follows:

*“I have to read a lot and stay updated and informed on the latest security threats and trends. I admit it is not very often or regular, and I must look for the time; otherwise, how will I protect my business and make informed decisions to do so?”*

Time constraints often impact decision-making, with SME owners juggling multiple responsibilities, making it difficult to dedicate regular time for detailed research on any SME challenge that will impact the security of the business. These challenges may shift their attention to vendors such as tech titans while seeking to foster business relations.

## **Transparency and Fair Practices**

The category transparency and fair practices emerged from one concept, ‘transparency and unfair advantage.’ Owners of SMEs will often advocate for transparency and the promotion of fair, ethical business practices to avoid being exploited by tech titans. SME owners feel that tech titans can manipulate information to suit their interests, pushing down SME search result content regardless of relevance to SMEs. For example, Participant #2 worries that specific algorithms run by tech titans can prioritize content that may create “filter bubbles.” This is mentioned as follows:

*“You know...? Some of these Big Techs [tech titans] rely on AI and algorithms to rank search results from our customers. They are a threat because they can unfairly display advertising and connect users at will; they have these algorithms that we do not know how they operate. I worry that they are unpredictable and can make things hard for small businesses to know how we can get our products to be seen by customers.”*

The lack of transparency may make it difficult for owners of SMEs to know how to use tech titan technologies to address their interests and reach their target audience. They feel tech titans may unfairly ‘game the system’, adversely impacting SME performance and customer reach.

## Advocacy and Empowerment

The category advocacy and empowerment emerged from two concepts, ‘advocacy’ and ‘empowerment.’ It was observed that owners of SMEs took a proactive approach to informing each other about regulatory environments such as the Protection of Personal Information Act (POPIA). As observed, this form of grassroots advocacy helped SMEs stay informed on changing InfoSec best practices. Participant #4 states as follows:

*“I prefer to stay informed and keep advocating to my business partners to stay up to date on regulatory changes related to data privacy. I understand POPIA is one of the recent regulatory requirements we must follow. This is one way to tell my business partners that we can have more control over our data and online presence.”*

SME owners recognized that they, too, were limited in terms of being aware of the InfoSec challenges, noting that they “do not have to go it alone.” This is an important step towards empowerment because it opens SMEs up to seeking assistance from each other. Participant #1 says the following:

*“I know that I do not have to go it alone when it comes to information security for my small business... I know I can take steps and seek help and resources to improve my situation and reduce reliance on Big Tech [tech titans]”*

It was observed that SMEs wanted to be proactive and take control of their InfoSec solutions by not waiting for others to solve their problems.

## Security and Privacy

The category security and privacy emerged from two concepts, ‘password hygiene’ and ‘data breach and privacy concerns.’ tech titans mandates their employees to undergo regular training on InfoSec best practices, such as password management. These enforce strong, complex, and unique passwords. Weak password hygiene contributes to a major InfoSec risk. This is especially so for SMEs. Participant #5 acknowledges the inconsistent training of password hygiene in the SMEs they own. They state,

*“I sometimes train my employees, depending on the time we must spare... yes, things like cybersecurity best practices and how to be aware of issues like phishing and good passwords ... I think it helps”.*

Stating “sometimes trains” may imply that they do not prioritize password management and may occasionally skip it due to time constraints. This may open the SMEs to InfoSec attacks. SMEs need to be aware of the risks posed by internal and external business partners and employees. SMEs should exercise concern regarding data breaches and privacy as crucial elements of a sound InfoSec posture. Sometimes, this understanding, as observed, is lacking within SMEs. Participant #4 acknowledges this by stating:

*“I sometimes rely on big tech platforms. This guy advised me on a solution, and I went for it. I was surprised I had limited control over how our data was collected by these big techs [Tech Titans]. I do not know how it is being used, which worries*

*me. What if there was a data breach on their end? I think this would impact us adversely.”*

Participant #4’s statement points to the need for SMEs to investigate how tech titans collect data and how it is used before undertaking any partnership or collaboration. Saying that “I was surprised to find out” demonstrates a poor understanding of tech titan platforms or third-party platforms, exposing the SMEs to privacy concerns. The following section discusses how SMEs may become resilient to InfoSec challenges and avoid the adverse consequences of tech titans managing business interests at the expense of SMEs.

## **Resilience and Taming the Tech Titans**

As pointed out by the study participants, SMEs can build resilience against InfoSec threats and carefully navigate through terrain where tech titans have competing interests. Participants mentioned password hygiene, privacy, InfoSec awareness, and secure data handling concepts. What was observed is the emotional and psychological toll these challenges have on the owners. For SMEs to remain resilient, they should prioritize a culture that fosters practical security measures and not become overly dependent on third parties. The study proposes a taxonomy of the categories elicited from the owners of SMEs into a framework that can guide and improve SMEs' InfoSec posture.

## **Taxonomy of Constructs**

For SMEs to remain resilient, they should prioritize a culture that fosters practical security measures and not become overly dependent on third parties. The study proposes a taxonomy of the categories elicited from the study participants. The taxonomy provides strategies for SMEs to

remain resilient and ‘tame’ the tech titans of business. A table of the taxonomy is presented in Table 5.

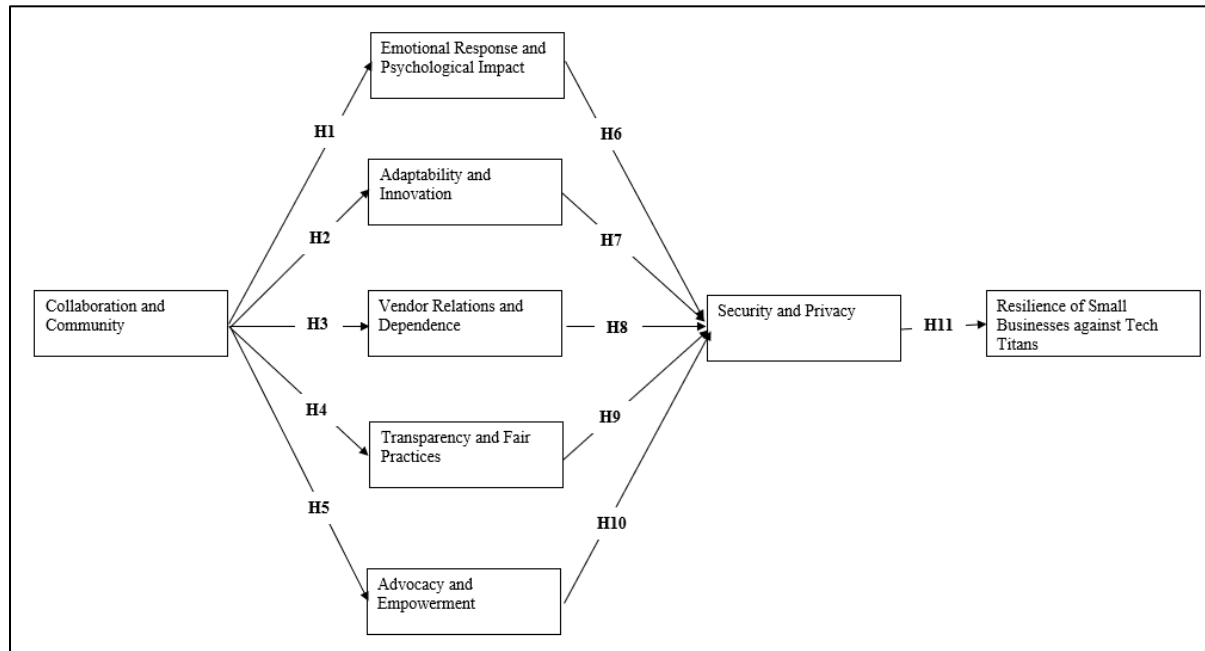
<b>Taxonomy of constructs</b>	<b>Resiliency strategies and taming the tech titan</b>	<b>Implementation</b>
Collaboration and Community	<ul style="list-style-type: none"> <li>• Create or join SME associations of business interest</li> </ul>	<ul style="list-style-type: none"> <li>• Create or join SME associations or online forums focused on InfoSec for SMEs.</li> <li>• Owners and/or employees to participate in knowledge-sharing events or workshops to explore joint initiatives and cost-effective security solutions.</li> </ul>
Emotional and Psychological Impact	<ul style="list-style-type: none"> <li>• Emotional well-being and psychological well-being</li> </ul>	<ul style="list-style-type: none"> <li>• Implement support systems like SME employee assistance programs (EPA) or stress management workshops.</li> <li>• Foster open channels of communication. Define InfoSec roles and responsibilities.</li> </ul>
Adaptability and Innovation	<ul style="list-style-type: none"> <li>• Constant learning and adapting to new challenges through technology and innovation</li> </ul>	<ul style="list-style-type: none"> <li>• SMEs may partner with universities and research institutions to access cost-effective expertise.</li> <li>• Tap into government funding and grants to these institutions</li> </ul>
Vendor Relations and Dependence	<ul style="list-style-type: none"> <li>• Vendor and third-party management</li> </ul>	<ul style="list-style-type: none"> <li>• SMEs should always review vendor agreements for InfoSec protocols for privacy and lock-ins.</li> <li>• Diversify vendor services to reduce or avoid dependency</li> </ul>
Ensuring Transparency and Fair Practices	<ul style="list-style-type: none"> <li>• Constantly promoting ethical business practices and holding tech titans accountable for exploitation</li> </ul>	<ul style="list-style-type: none"> <li>• SMEs can support local and regional regulatory efforts that promote transparency and fair practices within SMEs and other big businesses</li> <li>• Raise public awareness regarding bib business [Tech Titans] unfair practices through blog posts, newspapers, and other publication outlets.</li> </ul>
Advocacy and Empowerment	<ul style="list-style-type: none"> <li>• Nurture SME empowerment efforts and seek tools, resources, and authority to make impactful decisions.</li> </ul>	<ul style="list-style-type: none"> <li>• SMEs can participate in government initiatives and respond to policy proposals that impact the privacy and security of data.</li> </ul>
Security and Privacy	<ul style="list-style-type: none"> <li>• Implement best practice InfoSec standards for SMEs</li> </ul>	<ul style="list-style-type: none"> <li>• SMEs can implement best practices standards such as intrusion detection systems (IDS), data encryption, password hygiene, awareness of phishing, reporting suspicious activity, regular software updates, and carrying out security audits</li> </ul>



**Table 5. InfoSec Taxonomy of SMEs' Resilience to challenges. Source: Own compilation**

## Theory of InfoSec Resilience

The InfoSec resilience taxonomy discussed in the previous section was used to develop the theory of resilience by SMEs to address the challenges of InfoSec to ‘tame’ tech titans and the technologies they have developed, which can exacerbate InfoSec risks to these SMEs. This theory can be called the *SME InfoSec Resilience* theory. The theory draws from the categories identified in the GT method used in this study. In GT, theory development is the outcome of a grounded theory study. The GT method used in this study allowed the researcher to build a new theory based on data collected from the study participants. The study participants presented real-world settings and contexts in which SMEr-IS is built. *SME InfoSec Resilience* theory is presented in Figure 2.

**Figure 2:** *SME InfoSec Resilience* theory. Source: Own compilation

*SME InfoSec Resilience* theory proposes the following hypotheses.

**H1:** Collaboration and community will positively affect SME owners' emotional and psychological traits.

**H2:** Collaboration and community will positively affect the adaptability and innovation of SMEs.

**H3:** Collaboration and community will positively affect vendor relations and SMEs' dependency.

**H4:** Collaboration and community will affect transparency and fair practices within SMEs positively.

**H5:** Collaboration and community will affect the advocacy and empowerment within SMEs positively.

**H6:** Emotional and psychological impact will affect SMEs' security and privacy positively.

**H7:** Adaptability and innovation will affect SMEs' security and privacy positively.

**H8:** Vendor relations and dependence will affect SMEs' security and privacy positively.

**H9:** Transparency and fair practices will affect SMEs' security and privacy positively.

**H10:** Advocacy and empowerment will affect SMEs' security and privacy positively.

**H11:** Security and privacy measures will affect SMEs' resilience to tech titans positively.

The researcher acknowledges that *SME InfoSec Resilience* theory can be subject to various interpretations and may be limited as follows:

- The theory is provisional. This theory may be elaborated on or even refuted in its claims.
- The theory is limited in time. This theory may be influenced by a particular era or society (Strauss & Corbin, 1994, p. 279).

## MANAGERIAL IMPLICATIONS

As pointed out in the study, tech titans have a significant impact on the InfoSec posture of SMEs, sometimes adversely. Owners of these SMEs are InfoSec resilient to the adverse effects of tech titans only if they remain cautious of the InfoSec threats by the technologies that are often developed by these tech titans. These tech titans' reliance on solutions to these threats can harm SMEs. The detriments range from solutions that may not be compatible with SME needs to situations where SMEs may be locked into vendor products and services. SMEs can overcome these challenges by following the proposals stipulated by a taxonomy of resilience presented in this study. This taxonomy shows how SMEs can remain resilient and tame the tech titan. The taxonomy categorizes strategies into eight areas that can be applied to tame the challenges posed by, but not limited to, InfoSec threats and the tech titans' technologies and business practices that generate these threats. These eight areas include collaboration and community, emotional and psychological impact, adaptability and innovation, vendor relations and dependence, transparency and fair practices, advocacy and empowerment, and security and privacy. Each category offers a detailed approach to how SME owners and managers can build resilience. Understanding that SMEs will have difficulty building resilience by replicating everything that tech titans do, it remains paramount to prioritize implementable strategies stipulated in the taxonomy to protect their critical information infrastructure.

## CONCLUSION, STUDY LIMITATIONS AND FUTURE RESEARCH

As This study has addressed how SMEs can be resilient and tame the hostile business environment characterized by InfoSec threats and tech titans. The researcher has presented a taxonomy of strategies SMEs can implement to remain resilient. Using GT methods, the researcher elicited qualitative data that formed the basis of the *SME InfoSec Resilience* theory. The theoretical

propositions of this theory have been outlined in the form of 11 Hypotheses that can be tested quantitatively. Future research can focus on quantitatively testing *SME InfoSec Resilience* theory using a survey to support this theory.

## ACKNOWLEDGMENTS

I would like to acknowledge the efforts of the blind reviewers and editors whose valuable inputs have helped improve the quality of the paper.

## REFERENCES

- Abbas, J., Mahmood, H. K., & Hussain, F. (2015). *Information security management for small and medium size enterprises*. *Sci.Int*, 27, 2393-2398.
- Aliyu, M. B. (2017). Efficiency of boolean search strings for information retrieval. *American Journal of Engineering Research*, 6(11), 216-222
- Amini, M., & Jahanbakhsh Javid, N. (2023). A multi-perspective framework established on diffusion of innovation (DOI) theory and technology, organization and environment (TOE) framework toward supply chain management system based on cloud computing technology for small and medium enterprises. January 2023. *International Journal of Information Technology and Innovation Adoption*, 11, 1217-1234.
- Arroyabe, M. F., Arranz, C. F., de Arroyabe, I. F., & de Arroyabe, J. C. F. (2024). *The effect of IT security issues on the implementation of industry 4.0 in SMEs: Barriers and challenges*. *Technological Forecasting and Social Change*, 199, 123051.
- Baabdullah, A. M., Alalwan, A. A., Slade, E. L., Raman, R., & Khatatneh, K. F. (2021). SMEs and artificial intelligence (AI): Antecedents and consequences of AI-based B2B practices. *Industrial Marketing Management*, 98, 255-270.
- Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*, 27(3), 393-410.
- Bandari, V. (2023). Enterprise data security measures: A comparative review of effectiveness and risks across different industries and organization types. *International Journal of Business Intelligence and Big Data Analytics*, 6(1), 1-11.
- Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, 63(4), 531-540.
- Bolek, V., Láatečkováá, A., Romanováá, A., & Korček, F. (2016). Factors affecting information security focused on SME and agricultural enterprises. *Agris on-Line Papers in Economics and Informatics*, 8(665-2016-45137), 37-50.
- Bramer, W. M., De Jonge, G. B., Rethlefsen, M. L., Mast, F., & Kleijnen, J. (2018). A systematic approach to searching: An efficient and complete method to develop literature searches. *Journal of the Medical Library Association*: 106(4), 531.

- Carbonara, E., & Santarelli, E. (2023). *Artificial Intelligence and robots: a threat or an opportunity for SMEs and entrepreneurship?* In *SMEs in the Digital Era* (pp. 104-121). Edward Elgar Publishing.
- Carías, J. F., Borges, M. R., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). *Systematic approach to cyber resilience operationalization in SMEs*. *IEEE Access*, 8, 174200-174221.
- Charmaz, K. (2008). Reconstructing grounded theory. *The SAGE handbook of social research methods*, 461-478.
- Christopher, M. and Peck, H. (2004), “Building the resilient supply chain”, *International Journal of Logistics Management*, Vol. 15 No. 2, pp. 1-13, doi: 10.1108/09574090410700275.
- Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, 6(23), 31.
- Corbin, J., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative sociology*, 13(1), 3-21.
- Corbin, J., & Strauss A., (2014). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, (Sage, London).
- Davidson, G., & Majumdar, S. (2022). *Boolean logical operator driven selective data filtering for large datasets*. Paper presented at the 2022 Annual Modeling and Simulation Conference (ANNSIM), 824-838.
- Delgado López-Cózar, E., Orduña-Malea, E., & Martín-Martín, A. (2019). *Google scholar as a data source for research assessment*. *Springer Handbook of Science and Technology Indicators*, , 95-127.
- Draucker, C. B., Martsolf, D. S., Ross, R., & Rusk, T. B. (2007). Theoretical sampling and category development in grounded theory. *Qualitative health research*, 17(8), 1137-1148.
- Drydakakis, N. (2022). Artificial Intelligence and reduced SMEs’ business risks. A dynamic capabilities analysis during the COVID-19 pandemic. *Information Systems Frontiers*, 24(4), 1223–1247.
- Elhusseiny, H. M., & Crispim, J. (2022). SMEs, barriers and opportunities on adopting industry 4.0: A review. *Procedia Computer Science*, 196, 864-871.
- Fatoki, O., & Odeyemi, A. (2010). Which new small and medium enterprises in South Africa have access to bank credit? *International Journal of Business and Management*, 5(10), 128.
- Glaser, B., & Strauss, A. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Mill Valley, CA: Sociology Press.
- Goel, L., Russell, D., Williamson, S., & Zhang, J. Z. (2023). Information systems security resilience as a dynamic capability. *Journal of Enterprise Information Management*, 36(4), 906-924.
- Hernandez, C. A. (2009). Theoretical coding in grounded theory methodology. *Grounded Theory Review*, 8(3).
- Kayode-Ajala, O. (2023). Establishing cyber resilience in developing countries: An exploratory investigation into institutional, legal, financial, and social challenges. *International Journal of Sustainable Infrastructure for Cities and Societies*, 8(9), 1-10.
- Kosseff, J. (2016). Positive cybersecurity law: Creating a consistent and incentive-based system. *Chapman Law Review*., 19, 401.
- Kurpjuhn, T. (2015). The SME security challenge. *Computer Fraud & Security*, 2015(3), 5-7.
- Lamoureux, S. M., Movassaghi, H., & Kasiri, N. (2019). The role of government support in SMEs’ adoption of sustainability. *IEEE Engineering Management Review*, 47(1), 110-114.

- Matania, E., & Sommer, U. (2023). Tech Titans, cyber commons and the war in Ukraine: An incipient shift in international relations. *International Relations*, 00471178231211500.
- McCall, C., & Edwards, C. (2021). New perspectives for implementing grounded theory. *Studies in Engineering Education*, 1(2), 93-107.
- Mohseni, S. Z. (2022). *Network security for small businesses*. Metropolia. Available at [https://www.theseus.fi/bitstream/handle/10024/779956/Mohseni\\_Zakaria.pdf?sequence=2&isAllowed=y](https://www.theseus.fi/bitstream/handle/10024/779956/Mohseni_Zakaria.pdf?sequence=2&isAllowed=y). Accessed on 7/7/24.
- Moradi, M., & Dass, M. (2022). Applications of artificial intelligence in B2B marketing: Challenges and future directions. *Industrial Marketing Management*, 107, 300-314.
- Statistics South Africa (StatsSA) (2024), *Three facts about small business turnover in South Africa*, Department, Statistics South Africa Available at <https://www.statssa.gov.za/?p=13900> Accessed on 7/7/24.
- Strauss, A., & Corbin, J. (1998). Basics of qualitative research techniques.
- Serenko, A., & Dumay, J. (2015). Citation classics published in knowledge management journals. part II: Studying research trends and discovering the google scholar effect. *Journal of Knowledge Management*, 19(6), 1335-1355.
- Telo, J. (2019). A comparative analysis of network security technologies for small and large enterprises. *International Journal of Business Intelligence and Big Data Analytics*, 2(1), 1-10.
- Urquhart C. (2000) *An encounter with grounded theory: tackling the practical and philosophical issues*. EM Trauth, ed. Qualitative Research in IS: Issues and Trends (IGI Global) 104-140.
- Urquhart, C. (2019). *Grounded theory's best kept secret: The ability to build theory*. The SAGE handbook of current developments in grounded theory, 89-106.
- Webb, A. (2019). *The Big Nine: How the Tech Titans and their thinking machines could warp humanity*. Hachette UK.