The perceived impact of security and privacy risks on social commerce amongst social media users in South Africa

Samresh Ramjith

A research proposal submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business

Johannesburg, 2023

ABSTRACT

This research investigated the influence of social media attitude, social media trust, and risk awareness (cybersecurity and privacy) on social commerce intention. Five hypotheses were proposed, which were then tested with a sample of social media users via an online survey. Survey results were cleaned and then analysed through Partial Least Squares Structural Equation Modeling (PLS-SEM) using SmartPLS software. The study did not find a significant direct effect of social media attitude on social commerce intention, but did find that social media attitude was found to significantly influence social media trust. The moderation effects of cybersecurity risk awareness and privacy risk awareness on the relationship between social media trust and social commerce intention were not supported. The study supports and reinforces the importance of trust in social commerce and the need for businesses and social media platforms to continuously work to enhance trust amongst users. A research outcome is the necessity for deeper investigation into the role of user attitudes and risk awareness in social commerce. The study contributes to the social commerce literature by providing empirical evidence about the complex interplay between trust, attitude, and risk awareness, contributing to enhancing understanding of these relationships and their impact on business strategies.

KEYWORDS

Cyber security, privacy, awareness, South Africa, social commerce, digital commerce, cybercrime, PLS SEM.

DECLARATION

I, Samresh Ramjith, declare that this research report is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

Name: Samresh Ramjith Signature: SR

Signed at Midrand, Johannesburg

On the 6th of June 2023.

DEDICATION

This work would not have been possible without the support and encouragement of my wife and children who kept me motivated to continue, even during those rough moments when time is at a premium and energy levels are low. Getting this research over the line was just as import from an academic perspective, as it was to demonstrate to my children that they should never stop learning or attempting the difficult.

ACKNOWLEDGEMENTS

A huge “thank you” to Professor Brian Armstrong and the Wits Business School faculty for their inspirational lectures, drawing on real-world experience and contextualising it against the theoretical frameworks. Not only did this help drive understanding of the interplay between the two, but it also showed that the corporate and academic worlds are more deeply entwined than I would have first thought.

Thank you for Professor Thomas Dorson-Anning for his support as a supervisor to this research and for his great suggestions on improvements and deeper analysis.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

PLS – Partial Least Squares

SEM – Simultaneous Equation Modeling

VIF – Variation Inflation Factor

CHAPTER 1. INTRODUCTION

1.1 Statement of purpose

This research is a quantitative study of the perceived impact of cyber security and privacy awareness on a social media user's propensity to engage in social commerce.

1.2 Background of the study

The COVID19 pandemic dramatically accelerated the adoption of digital technologies by corporates and consumers alike, with some estimates suggesting a staggering 7 years of implementation efforts condensed in to the COVID19 period (McKinsey, 2020). With restrictions on travel and movement, many ordinary citizens resorted to the use of social media and online tools to maintain contact with the outside world. In South Africa, social media usage increased by 12,00% from 2021 to 2022, with the user base now at approximately 28 million user or just under 50% of the country's population (Kemp, 2022), with an anticipated 40,77 million users by 2026 (Statista, 2022).

This growth in social media consumption in South Africa is in turn, driving an increase in social commerce. Social commerce is essentially the use of social media platforms, such as Facebook, Twitter, and Instagram to promote and sell products or services, with consumers of using electronic word of mouth techniques available on the platform, such as sharing, liking, and retweeting to amplify the marketing of these products (Dollarhide, 2022). Social commerce can thus be viewed as a subset of digital commerce, using base features of the social media platform to promote and support product discovery, purchasing and fulfilment. In South Africa, the increase in internet usage and digital commerce is mirrored by an increase in cybercrime, with the country now ranking as the 6th highest globally by cybercrime density (SurfShark, 2021) with an increase from 11,8 victims per million internet users in 2016 to 50,8 victims per million in 2021.

The most prevalent types of financial cybercrimes include investment fraud, online payment scams, identity theft and credit card fraud (SurfShark, 2021).

While digital commerce attempts to assure users of trustworthiness using signals, such as independent security certifications, secure ecommerce payment platforms and physical world customer service, many of these mechanisms are not available or implemented in social media channels and are thus not available in social commerce (Kimery & McCord, 2006). This paradigm creates opportunity for cybercriminals with potentially no recourse for social commerce fraud victims. Social commerce appears to be a topic of sparse research, with social commerce cybercrime more so. A gap exists within current local knowledge to explore user awareness of these cyber security and online privacy threats in the context of social commerce and to determine user's risk appetite to utilise social commerce given the perceived higher risk associated with this type of transaction.

1.3 Research problem

Given the growth in internet penetration, digital commerce, social media and now social commerce in the country (Statista, 2022) (World Bank, 2022), it stands to reason that cyber criminals will be intent on exploiting a relatively naïve user community for profit (Business Insider, 2020). South Africa was ranked 56th in the world in the International Telecommunications Union's Global Cybersecurity Index, with neighbouring Mauritius ranked 4th and both Kenya and Rwanda ranked higher (ITU, 2019), indicating that while progress is being made, the country is still vulnerable from a cyber security perspective. An increase in online fraud and losses will create a downstream ripple effect on banks, credit providers and other service providers (Niekerk, 2017) which could negatively impact economic growth. Online commerce already is, and social commerce could prove to be, a valuable channel to expand supply chain reach and to provide goods and service outside of urban centres. Eroding trust in the digital commerce space could cause the country to retrogress in terms of global competitiveness, technology advancement and miss opportunities for economic growth.

While much literature exists around cyber security in Africa (Sutherland, 2017) (Gcaza & Solms, 2017) (Mabunda, 2021) (Sutherland, 2017) (Kshetri, 2019), the use of social media in Africa and on social commerce, very little exists around the interrelationship among social media attitude, social media trust, social media commerce and security and risk awareness indicating a gap in knowledge that this research aims to explore.

Recent research around the relationships between digital privacy and data sharing in the UK insurance sector (Blakesley & Yallop, 2019) showed that convenience and financial reward were initial extrinsic motivators for data sharing amongst consumers. Intrinsic motivators including fulfilment of the transaction, maintaining control of their data and not having their personal data used to the detriment of the participants. However, concern around privacy issues were generally low, provided that antecedents conditions were met. Work by (Mutambik, Lee, Almuqrin, Zhang, & Homadi, 2023) defined three distinct factors that combined to underpin a user's privacy concerns in relation to social commerce:

- CUPI – the Collection and Use of Personal Information,
- PCPI – the Personal Control of Private Information,
- AAPP – the Awareness and Acceptance of Privacy Policy.

They also found that cultural factors played a role in the overall impact of privacy on social commerce intention. (Yerby & Paliszkiewicz, 2019) studied the link between a user's risk beliefs and their privacy concerns in social media and concluded that the risk concerns are valid, which means that social media sites need to recognise the need for and implement privacy measures to protect user information. In addition, social media sites need to provide the tools for users to manage their information on social media sites, and also alert users to privacy breaches.

1.4 Research objectives

This adoption study sought to:

1. Determine the extent to which Social Media Attitude influences social commerce intention
2. Analyse the influence of Social Media Attitude on social media trust
3. Examine the relationship between SM trust and Social Commerce Intention
4. Determine the extent to which the relationship between SM trust and SCI is moderated by cybersecurity risk awareness
5. Determine the extent to which the relationship between SM trust and SCI is moderated by privacy risk awareness

1.5 Research significance

In South Africa, the increased internet penetration to 70% of the population in 2020 (World Bank, 2022), especially by mobile users, and the increasing adoption of digital commerce by new entrants and traditional brick and mortar retailers, exceeds consumer awareness of the associated security and privacy threat vectors, which potentially explains the marked increase in victims per million over the past 5 years (SurfShark, 2021).

This adoption study approached the topic from the perspective of South African social media users who may or may not be engaging in social commerce to determine whether the perceived security and/or privacy risks influence their propensity to engage in social commerce. An understanding of the social media user's awareness level could assist social commerce accounts in determining what signals would be required to build trust with users and in turn potentially reduce fraud. This would have the benefit of potentially reducing online fraud, cybercrime, and privacy related incidents. Social commerce accounts may be able to provide these signals directly, potentially independent of the platform provider which could support commercial outcomes to the benefit of the provider. This win-win is vital in supporting social commerce as a viable, sustainable long term business model.

One of the most significant outcomes of the study is providing deeper insight to the usage of social commerce in South Africa. Much of the theoretical framework of this study relies on work conducted in other developing markets indicating a potential knowledge gap in the local market. In addition, a better understanding

of the moderating effect of user perceptions and awareness of security and privacy on social commerce, social media sites operating in South Africa can take steps to improve user practices, e.g., by enforcing stronger passwords or multi-factor authentication and creating more transparent privacy practices that allow users better control of their personal data, which could in turn reduce fraud and the exploitation of other security and privacy risks.

1.6 Delimitations of the study

The boundaries of the study are:

i. The respondent group will comprise South African social media users.
ii. Respondents completed an online survey, with no face-to-face interaction.
iii. Survey questionnaire was in English and not translated to other languages.
iv. No personal data was equired to complete the survey, except for broad demographic data.
v. Formal interpretation of the respective social media platform's terms and conditions was out of scope.

1.7 Definition of terms

Term	**Definition**
Cyber security	The system of people, processes and technologies that combine to protect information technology networks, equipment and software from malicious attacks that may compromise the ability of the system to function, reveal sensitive data or produce accurate computational results. (Kaspersky, 2022), (ITGovernance, 2022), (CISA, 2019)

Data/Information/Online privacy	The right of a data subject, which could be a natural person or juristic entity, to control the way their personal information is used when conducting activity on the internet. (IAPP, 2022), (NIST, 2022), (Protection of Personal Information Act 4 of 2013, 2022)

1.8 Assumptions

The research assumptions include:

- Environmental factors such as time of day and mental state across respondents will be statistically neutral.
- Respondents will answer honestly, with no bias or intent to skew results.

1.9 Chapter Outline

Further chapters in this report are structured as follows:

- Chapter 2 presents the Literature Review and Theoretical Framework.
- Chapter 3 presents the Research Methodology.
- Chapter 4 presents the results of the research.
- Chapter 5 discusses the results in relation to existing research.
- Chapter 6 presents the summary and conclusion.

CHAPTER 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Introduction

This structure of this sections is as follows: next is a review of the theoretical framework, followed by a discussion of some of the background context from existing literature relating to social media, social trust, and issues related to the security and privacy of these platforms, followed by hypotheses development.

2.2 Theoretical Framework

Existing research theories suggest a strong link between personality traits and user attitudes to social media, with (Horzum, 2016) suggesting five major factors, namely: Neuroticism, Extraversion, Openness to experience, Agreeableness and Conscientiousness, as the overarching variables that shape a user's perception, usage, and trust of social media platforms. These factors exist on a spectrum from high to low, e.g. extraversion to introversion.

Work by (Horzum, 2016) supports the five-factor model and adds Competency and Familiarity to the mix. (Ngai, Tao, & Moon, 2015) expand on this socio-psychological base by viewing the five-factor model as part of a wider group of personal behaviour theories, social behaviour theories and mass communication theories. Their framework seeks to contextualise the user's perception of social media in the context of endogenous motivation factors, such as personality traits, technology acceptance, reasoned action, and planned behaviour.

This singular context is affected by exogenous factors such as social influence, social interaction, social involvement, and social loafing to which also play a role in biasing the user's perception and behaviour on social media. These societal level behaviours are in turn shaped by para-social interactions & users and gratifications theory. Thus, a user's trust, perception and behaviour on social media is the result of a complex interplay amongst endogenous and exogenous

factors in both the physical and virtual worlds. The (Ngai, Tao, & Moon, 2015) do not consider factors such as security, privacy as standalone concepts but instead group these as part of a mediating group termed “tool integrity”.

Social psychology suggest several behavioural theories interact in a complex, nuanced manner in social media engagement and social commerce intention, notably:

1. Theory of Planned Behavior (TPB): This theory posits that an individual’s intention to engage in a behavior influenced by attitudes toward the behavior, subjective norms, and perceived behavioral control (Azjen, 1991). In the context of social media, TPB can be used to predict how likely individuals are to engage in social media activities based on their attitudes towards social media, the influence of their social circle, and their confidence in their ability to use social media (Zhang, Guo, Hu, & Liu, 2017).
2. Social Cognitive Theory (SCT): which posits that people learn by observing others and their environment (Khang, Han, & Ki, 2014). In social media, users learn and imitate the behavior of others. For example, seeing friends or influencers engaging in social commerce could increase an individual's intention to do the same. (Hajli, 2012)

(McFarland & Ployheart, 2015) build on this physical-virtual entanglement in their Omnibus Context Continuum Model, depicted in figure 2 below, which suggests that social media is subject to the same discrete stimuli and psychological theories as other digital communication and physical interactions, i.e., a user’s social media behaviour is influenced (and influenceable) by the same building blocks as other communication interactions.

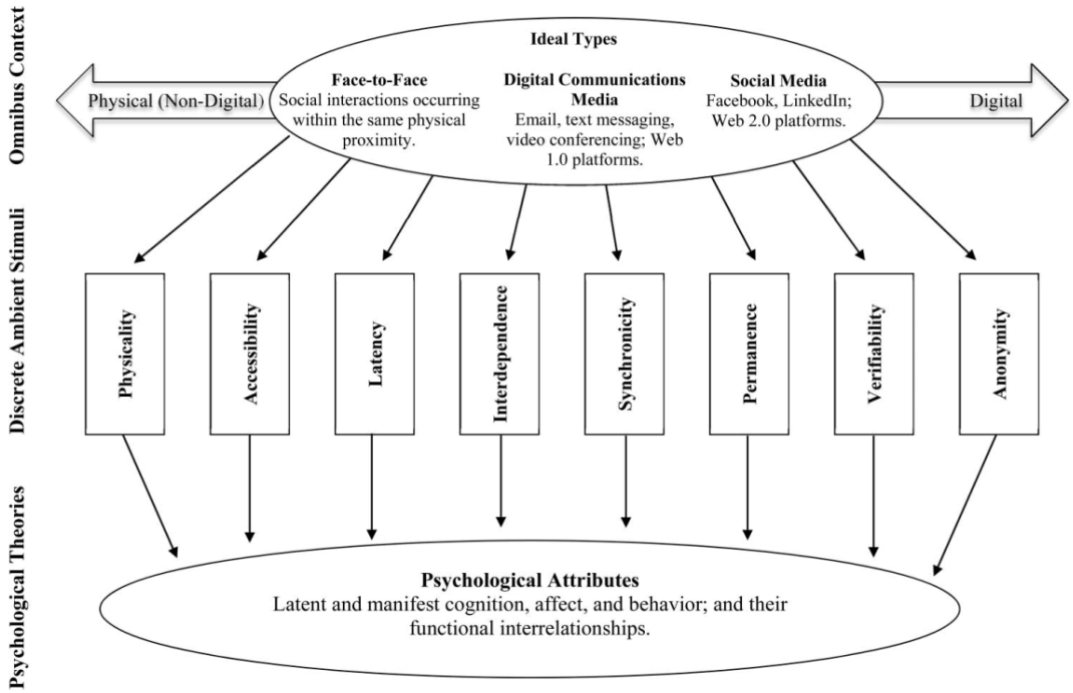

Figure 1 - Omnibus Context Continuum Model

The Omnibus Context Continuum Model does include “Anonymity” as a building block, but in the context of a user viewing their social media interactions as being anonymous, which suggests that social media users could view online privacy as an implicit component of the social media platform and harbour an expectation of privacy by default.

(DülekIbrahim & aydın, 2020) found significant relationship between social media marketing and brand loyalty, meaning that social media users are quite likely to utilise social commerce as they are physical channels for purchase fulfilment, but did not study direct linkage between social media marketing and intention to purchase. (Chow & Shi, 2014) found that social media users build and evaluate social commerce trust across two dimensions, namely, information-based, and identification-based. Hajli’s Social Commerce Adoption Model (Hajli, 2012) ties these factors to together and showed that positive social media attitude positively influenced social media trust, which in turn positively influenced the user’s propensity to engage in social commerce.

Studies illustrate the impact of trust as a moderator on digital commerce, with (Rios & Riquelme, 2010) finding that user's inability to trust a website as significant deterrent to online commerce and restricts brand engagement. (Ilmudeen, 2019)'s work showed that privacy, security and trustworthiness positively contribute to digital commerce adoption, while (Wang & Herrando, 2019) found that users expect social commerce sites to integrate privacy, security and facilitate trust on their platforms. Study by (Ayaburi & Treku, 2020) examined the effect of penitence by social media platforms in the wake of data breaches, which showed that trust repair is dependent of the nature of the relationship between the user and the platform.

2.3 Conceptual Framework

When the first email was sent in 1971, few people at that time could have imagined the civilization changing impact that computing and computers would have at almost every level of society, globally. Today computers are built into the fabric of our everyday existence – from smart buildings, smart cars and smart appliances to the systems that help design and manufacture nearly everything we use in our day to day lives (Singer & Friedman, 2014). Initially isolated, computer systems were networked to form the internet, and now tiny, embedded sensors and devices are being connected to the internet, leading to an exponential increase in the amount of data being produced, and in the number of connected devices accessible from nearly anywhere in the world. This "Internet of Things" (Ranger, 2020) is rapidly becoming a communication fabric connecting the physical and virtual worlds.

Just as the infrastructure of the internet is changing and evolving, so too are the applications that execute over the internet. Social media, which is an information technology-based channel for internet users to create, curate, share and exchange digital content is amongst the most frequently and largely used technologies of the modern digital society (USF, 2022), (Kaplan, 2018) with more than half of the world's population engaging on social media platforms daily.

Social media itself has evolved (Ortner, Sinner, & Jadin, 2018) from initially being text-based services to include:

- Global platforms like Facebook, Twitter, LinkedIn, Instagram, and Tumblr,
- Micro-blogging sites,
- Video blogs such as YouTube, TikTok and Vimeo,
- Non-internet facing corporate platforms such as Workplace,
- Forums and chatrooms,
- And other more niche regional and community-centric groups.

Figure 1 below depicts the ranking of the most popular social media platforms, according to Hootsuite's 2022 survey (Hootsuite, 2022). While the Meta company's brands (Facebook, WhatsApp, Instagram) dominate due to popularity across the United States and Europe, niche Asian-centric platforms such as QQ, Sina Weibo and Douyin enjoy significant supports in their respective markets.

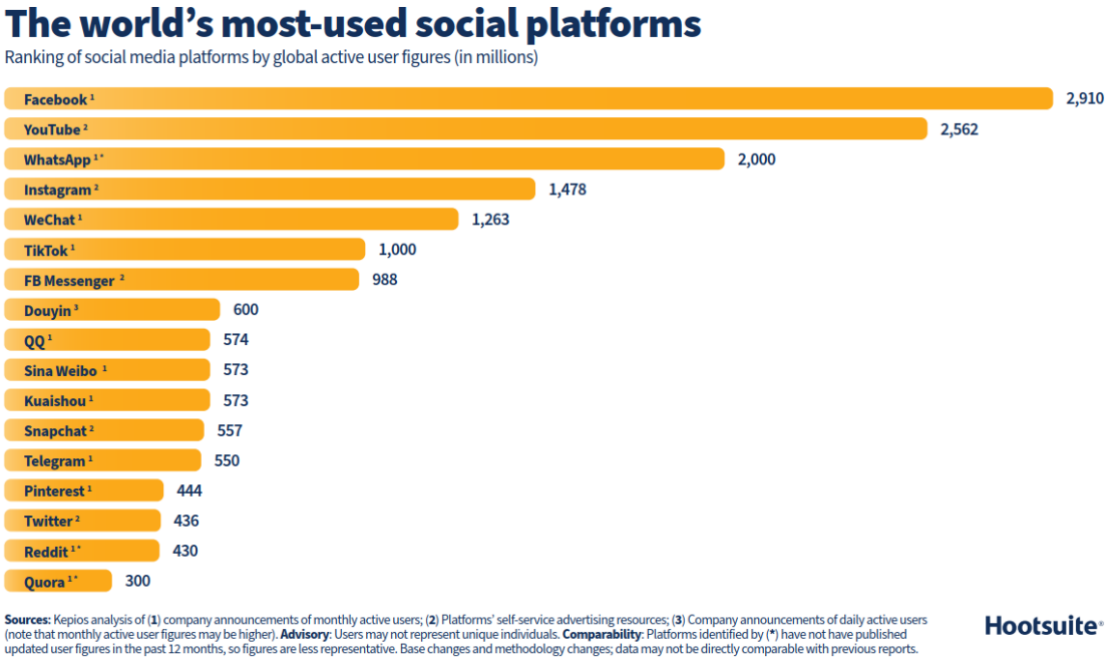

Figure 2 - social media platform rankings

With this audience reach, the evolution to using these platforms to market and sell products seems a natural progression. One of the factors driving the growth of social commerce is the shift in marketing strategy from attracting new customers, to relationship-based customer engagement, lifetime customer value and ongoing customer interactions (Salvatori & Marcantoni, 2015). Given the

strong customer affinity for social commerce, two main drivers are evolving the social media landscape:

1. Social media features being developed and incorporated in traditional digital commerce platforms,
2. Existing social media sites adopting and developing digital commerce capabilities, e.g., Facebook Marketplace.

South African consumers are following the social commerce trend (Mzekandaba, 2021) with Generation Z consumers in the 25 year old to 40 year old demographic being the fastest growing group, using Facebook, TikTok and Instagram for their online shopping, with the local market expected to grow at a rate of approximately 62% to over $833 million in 2022 (Research and markets, 2022). Consumption of social media and social commerce on mobile devices is the fastest growing channel across Europe, Middle East, and Africa (EMEA) leading to simultaneous adoption of social media and social commerce by the newly connected (Lowes, 2021). However, Lowes cites consumer trust in social commerce payments as one of the major barriers to growth, with safe and secure payments being seen as a significant factor in the growth of social commerce in South Africa.

Social commerce security risks include (Khidzir, Ismail, Daud, Ghani, & Ibrahim, 2016) (SurfShark, 2021):

1. Identity theft – in which a malicious third party uses customer information to create a fake profile impersonating the customer to commit fraud. This brings the authentic customer into disrepute, with impacts on credit worthiness, payments, and potential long-term reputational consequences (USAGov, 2022)
2. Financial cybercrime including investment fraud, online payment scams, and credit card fraud.
3. Legal transgressions – which in South Africa is based on the regulatory changes within the South African legislative environment with the introduction of the Protection of Personal Information Act (POPIA) which was signed into law on 1 July 2020 (Michalsons, 2022) and the Cybercrimes Act, which came into effect on 1 June 2021 (Grant Williams, 2021) (Ellipsis, 2021). While the POPIA act focuses on the rights of data subjects and related personal information, the Cybercrimes act defines and imposes penalties for cybersecurity related offences.

In addition, social media platforms impose their own legal frameworks on the use of their products and acceptable usage policies in terms of content and form. All three of these factors interplay in determining the context of the interactions of interactions with and on social media platforms, which could have impact on the user's trust relationship and propensity to conduct social commerce on a given platform.

The social media platform forms the ecosystem for the social commerce transaction, with social media trust, i.e., product reviews by other social media users, electronic word of mouth, and other positive sentiments towards a supplier or product creating the positive catalyst to engage (Sohaib, 2021). Cyber security and Privacy risks would be the moderating variables that strengthen or weakens the purchaser's social commerce intention. Social commerce intention is the aggregate result of a customer evaluating the benefits and risks of paying for a product or entering a transaction (Othman, et al., 2019). The relationships between these variables are depicted in figure 2 below:

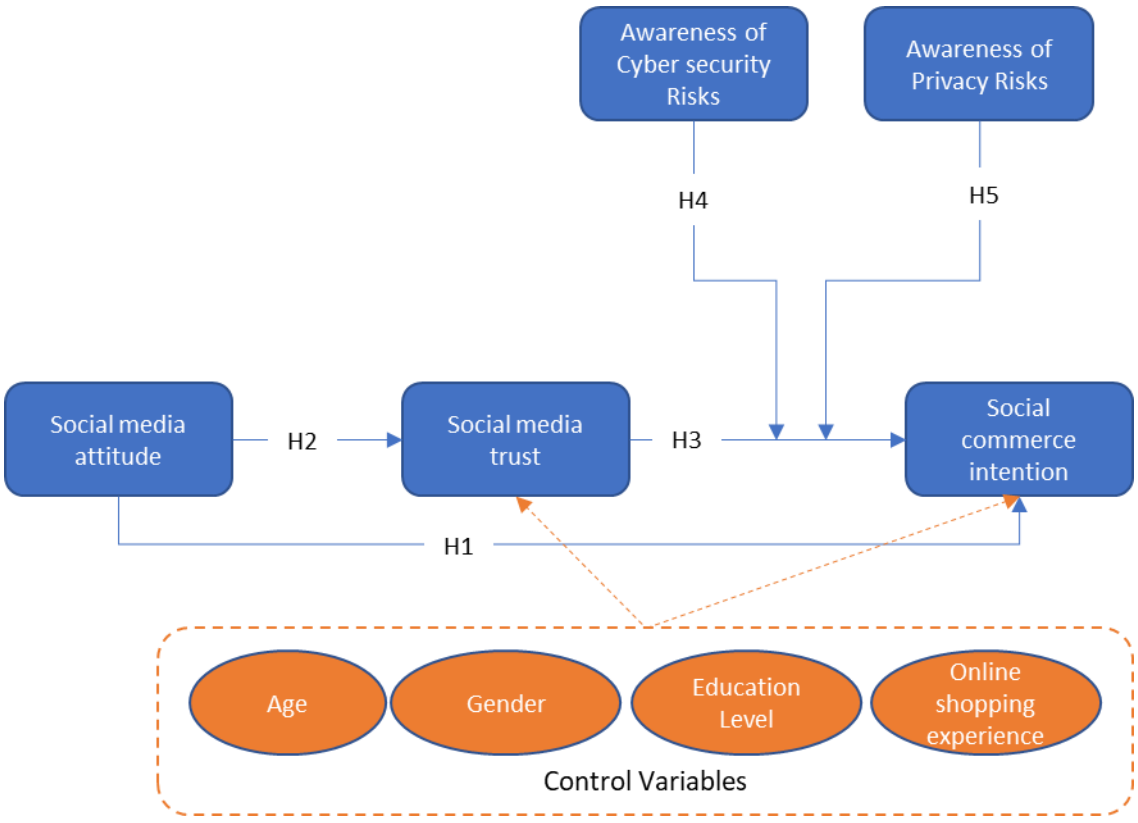

Figure 3 - Research conceptual framework

Studies have shown strong links between social media and digital commerce where brand and product perceptions, influence on buying decisions and exposure to new products are shaped by conversations on social media (Anjum, 2019). Social commerce then is the process of buying and selling products directly on social media sites (Bölükbaşı, 2021).

Social commerce, while a subset of digital commerce, differs from traditional business-to consumer, business-to-business and derivative models by occurring entirely on a social media platform, outside of a traditional digital commerce platform, such as Amazon, Takealot or Alibaba (Wang C. &., 2012). One of the factors driving the growth of social commerce is the shift in marketing strategy from attracting new customers, to relationship-based customer engagement, lifetime customer value and ongoing customer interactions (Salvatori & Marcantoni, 2015). Given the strong customer affinity for social commerce, two main drivers are evolving the social media landscape:

1. Social media features being developed and incorporated in traditional digital commerce platforms,
2. Existing social media sites adopting and developing digital commerce capabilities, e.g., Facebook Marketplace.

These factors are collectively known as Social Trust, which creates a positive effect on the user's intention to purchase via social commerce platforms. This effect produces Hypothesis 1:

H1: social media attitude positively influences social commerce intention.

In addition, users may harbour reputational perceptions of different social media platforms, and their attitude towards the platform may impact their trust level of that platform. This trust level then influences the user's willingness to engage in social commerce and the degree (amount of spend) in which the user is willing to engage. Research in Indonesia (Ashoer, 2016) identified several risks to influencing the customer's intention to purchase in digital commerce, including:

1. Financial risk – which relates to paying more for a product online as opposed to in a brick-and-mortar store, as well as potential fraud losses.

2. Time risk – lost time due to inefficiencies in the purchasing process, such as finding products or transaction delays.
3. Social risk – the risk of the purchased product affecting others' perceptions of the purchaser,
4. Product risk – where the product does not function or perform as advertised or expected,
5. Delivery risk – which refers to challenges with forward logistics and ultimate delivery to the customer,
6. Security and Privacy risk – where the customer's personal information is misused or abused by either the platform or malicious third parties with access to the customer's information,
7. After-sale risk – defined as latent risks such as guarantee claims, fraud, or damaged goods post purchase.

South Africa's ranking as the 6th highest globally by cybercrime density (SurfShark, 2021) means that the Security & Privacy risk outweighs the other risk types across transactions and platforms and thus forms the key risk being evaluate in this study. Since social media allows user to share information about their social commerce experiences, product choices, post purchase experiences, some of these risks may be offset through the electronic word of mouth effect (Dinulescu, Visinescu, Prybutok, & Sivitanides, 2021).

The interplay of these risks and attitudes produces Hypothesis 2 and 3:

H2: social media attitude positively influences social media trust.

H3: social media trust positively influences social commerce intention.

Since social commerce is based on the use of social media platforms as the basis for transacting, many of the social media security risks directly impact social commerce. These risks include (He, 2012):

1. Poor authentication controls – most social media users utilise a simple username and password to control access to their online accounts. This simple combination can be guessed through random password attempts or though brute force and dictionary attacks that attempt thousands of passwords to break into the user's profile. Once access is gained, the attacker will change the user's password to one of his own choosing (to lock the legitimate user out) and can then impersonate the user online.

This will also give the attacked access to stored payment credentials and the ability to target the legitimate user's social network in further attacks.

2. Phishing & Spear-phishing – are emails that attempt to trick the recipient into clicking on a link that directs the user to a malicious website or opening an attachment that executes an attack. While phishing refers to a general broadcast of these types of emails, spear-phishing refers to more targeted emails, that often utilise information about the target group or recipient based on social media and other publicly available information. This profiling attempts to impersonate legitimate communication that the target would more likely trust.
3. Social engineering – relies on the exploitation of trust relationships that exist between users in a social network to propagate malicious software (or links to these) and misinformation/disinformation to persuade the user's social network toward a particular course of action. The attacker will often utilise shortened URLs to mask the true destination of an embedded link from the user, thus allowing for attacks that exploit the user's browser or operating system to install malicious software on the user's device, if vulnerable.
4. Web application attacks – which are directed at the software supporting the social media platform itself, should vulnerabilities in the platform's code be discovered. These attacks may also allow the use of infected plugins that steal user data or monitor the user's online activity and then attempt to extort money from the user to prevent this information being made public.

Knowledge and awareness of security risks on social media platforms may be a cause for concern that limits a user's propensity to engage in social commerce. This is the basis of Hypothesis 4:

Hypothesis 4: the relationship between social media trust and social commerce intention is moderated by cyber security risk awareness.

Selling advertising is one of the principal revenue generation mechanisms of the largest public social media platforms, such as Facebook, Twitter, and Instagram (McFarlane, 2021). Advertisers pay to target specific audiences – who are algorithmically profiled by the platform on a range of data points, including geographic location, age, gender, education, sexual orientation, political views, hobbies, likes/dislikes, potential income bracket and other details in the hope of increasing return on advertising spend (Leetaru, 2018), and reducing wasteful advertising. These initial "targeted" advertisements have evolved to adapt as a

user's behaviour changes – for example, based on the users' browsing habits or search history or relationship status change – to serve different, potentially more relevant advertisements, called "behavioural advertising" (Squires, 2016). It is in the social platforms interest to mine as much information as possible on each user – across platforms, and each user's social network – to increase the effectiveness of behavioural adverts and thus increase the number of paying advertisers on the platform.

Social media users are encouraged to participate by producing content, sharing content, or engaging with other users and brands to elicit more insight on the user and thus produce more data for the advertising algorithms (Mitrou, Kandias, Stavrou, & Gritzalis, 2014). The sheer scale of data collection by social media platforms creates significant privacy risk. Privacy relates to the degree of control the granted by the social media platform to its users over data collection, usage, sharing and destruction (Bansal & Chen, 2011). The key privacy concerns on social media and in social commerce relate to:

1. Excessive data collection (beyond that required to complete a transaction).
2. Unauthorised access to user information by third parties – either through information sharing beyond what the user anticipated or through malicious threat actors,
3. Secondary usage of user data for purposes other than what was originally intended or disclaimed,
4. Errors in user data that could lead to unintended consequences or data exposure.

While much debate exists around whether privacy is a tradable commodity or an inalienable human right, users still wish to control their personal information (Ackerman & Donald T. Davis, 2003). Social media platforms are also prized targets for cyber-attacks, given the density of user information available, as evidenced by some of the largest data breaches on record (Hill & Swinhoe, 2021):

1. Facebook (now Meta), breached in April 2019, with more than 530 million user records comprised,
2. LinkedIn, breached in June 2021, with approximately 700 million user records compromised,
3. Sina Weibo, breached in March 2020, with 538 million user records exposed.

In addition to the direct identity theft consequences of these breaches, these user records may remain indefinitely on the dark web, allowing attackers to repackage the data for use in spam, fraud, and other malicious activity. As social commerce grows, exposure of credit card and payment information as well as physical location information of customers will become more likely, increasing the risk of real-world consequences.

With the Protection of Personal Information Act of 2013 (POPIA) now enacted into South African law, the social media platform's ability to protect the privacy of South African users is also a critical requirement. The POPIA act allows users the ability to control the sharing of their personal information, request that a social media platform removes all their history and stored data and/or share all collected data on the user, amongst other rights (Government Gazette, 2013) (Simpson Attorneys, 2021). POPIA essentially aligns the South African data privacy regime with that of other privacy aware countries and regions such as Ghana, Kenya, the United Kingdom, Australia, India, and Europe, all of which have their own data privacy laws also applicable to social media platforms.

Based on this analysis, privacy risks may be a limiting factor to social commerce intention. This is the basis of Hypothesis 5:

H5: the relationship between social media trust and social commerce intention is moderated by privacy risk awareness.

2.4 Conclusion of Literature Review

In summary, the aim of the research was to explore the impact of the different risks on the social media user's perceived trust of the platform and whether this trust relationship will have any perceived impact on the user's propensity to conduct social commerce on the platform.

The following hypotheses were tested:

H1: social media attitude positively influences social commerce intention.

H2: social media attitude positively influences social media trust.

H3: social media trust positively influences social commerce intention.

H4: the relationship between social media trust and social commerce intention is moderated by cyber security risk awareness.

H5: the relationship between social media trust and social commerce intention is moderated by privacy risk awareness.

CHAPTER 3. RESEARCH METHODOLOGY

3.1 Research approach

This was primarily a phenomenological study, which sought to determine the magnitude, strength and direction of the relationships and hypotheses presented in the conceptual model. From this quantitative view, the study could draw conclusions to confirm the validity of the hypotheses and model. The study utilised a survey to collect data related to each hypothesis from a wide audience, across a large target group in a cost-effective manner. The survey itself comprised assertions, linked to numerical, quantitative values for analysis using structured equation modelling for model fit and confirmation or rejection of the hypotheses. Structured equation modelling was selected due to its ability to quantify and measure inferential data, while accounting for measurement error.

3.2 Research method choice

This quantitative study utilised open ended assertions, linked to a 5-point Likert scale to assess social media user's attitudes to the concepts of social media attitude, social media trust, it's impact on social commerce intention, security, and privacy.

3.3 Research time horizon

Due to time constraints, this study was a cross-sectional snapshot of the respondents between January '23 and February '23 as per the research project plan.

3.4 Research techniques and procedure

1.1. Population and sample

The target population for the study were South African social media users, who intended on or were already engaging in social commerce. The sample for this study was English language social media users who were reachable via Facebook, Twitter, Instagram, and LinkedIn platforms. The sample group was not constrained in terms of gender, ethnicity, income group or geographic location. The research context and link to the assessment was posted on Facebook, Twitter, Instagram, and LinkedIn inviting social networks connections to complete the survey. Respondents were encouraged to share the link to their networks to increase coverage and the sample size. The aim was to survey as wide and diverse a sample within South Africa as possible to facilitate the detection of trends or themes across the responses. Distribution via social channels provided the added advantage of immediately engaging users who were already on social media.

1.2. Data collection instrument

The primary data collection instrument was an online survey, with structured questions per thematic area. These responses were input to a numeric result that was tabulated per question to provide a score per thematic area and sub-area. Initial survey questions determined biographical data to allow isolation of the target group during data analysis. Consideration was given to the time taken to complete the survey to balance user participation, survey completion, and result quality. Draft versions of the questionnaire were tested with a small sample group comprising cyber security and privacy experts from the researcher's professional network to fine-tune questions and provide insight to more meaningful outcomes-based and scenario-type questions. This pilot phase also allowed for the testing of the data capture and output of the Qualtrics platform to ensure that results

would be exportable for data analysis in a manner that minimised the risk of errors.

1.3. Measures

The scales of the assessment incorporate existing questions from (Ross, et al., 2009), (Molinillo, Liébana-Cabanillas, & Anaya-Sánchez, 2018) and (Ayaburi & Treku, 2020). The security and privacy scales are adapted from the National Institute of Science and Technology (NIST) cybersecurity framework (NIST, 2018).

The assertions were measured against a 5-point Likert scale, ranging from “strongly disagree” to “strongly agree” with a numeric score (from 0 to 5) for each rating level. The assertions form the basis of the formative measurement model used in the PLS SEM calculation. These formative indicators were then grouped per thematic area which in turn are used as the composite endogenous variables in the PLS SEM structural model.

1.4. Data analysis

Considering the exploratory nature of the research, PLS SEM (Partial Least Squares Simultaneous Equation Modelling) was the preferred data analysis option for this study. (Hair, Matthews, Matthews, & Sarstedt, 2017). The numerical data produced by the surveys was analysed using PLS SEM techniques to determine the correlation between the variables presented by the hypotheses and the observed results. PLS SEM was a good fit as it allowed the simultaneous examination of both the path(structural) and factor (measurement) models in one model (Alshibly, 2015). PLS SEM is also more powerful than regression analyses and provides a framework to test the validity of theory using empirical models while simultaneously accounting for measurement errors (Beran & Violato, 2010). Smart PLS software was used to analyse the data against the multivariate model. While sample size is a SEM consideration, PLS SEM lends itself to accuracy with smaller sample sizes (Hair, Matthews,

Matthews, & Sarstedt, 2017). From (Chin, 1998), the sample size should be 10 times the number of items related to the most complex variable or construct. The conceptual model presented contains 5 variable and 5 constructs, which means the calculation will require a minimum of 50 responses to produce valid results.

In addition, age, gender, education level and online shopping experience are included as control variables that impact social media trust and social commerce intention (Sohaib, 2021).

Evaluation of the PLS SEM model followed a structured procedure (Hair J. , Hult, Ringle, & Sarstedt, 2022):

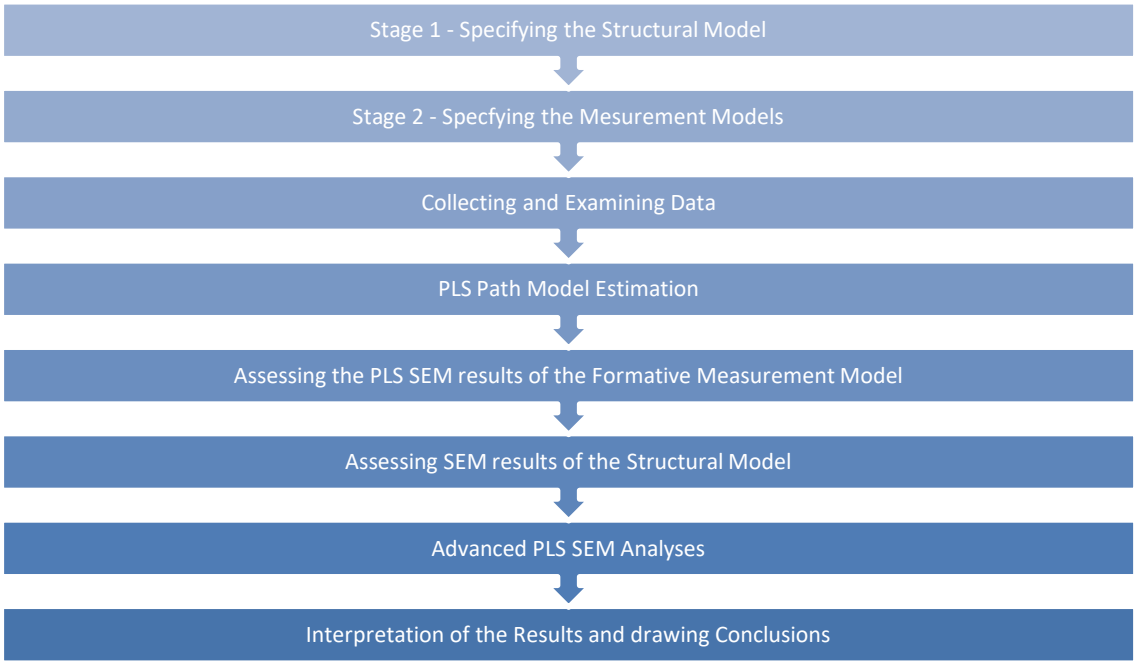

Figure 4 – PLS SEM evaluation procedure

1.5. Reliability and validity

Evaluation of a formative PLS SEM result follows a two part process (Hair J. , Hult, Ringle, & Sarstedt, 2022):

1. Evaluation of the structural model, which indicates the relationship between the constructs (inner model),

2. Evaluation of the measurement model, which indicates the relationship between the constructs and indicator variables (outer model).

Each of these phases considers the statistical relationships between the element to determine the statistical significance and data reliability during each phase of the evaluation. The figure below outlines the steps followed in assessing the reliability of the formative model (Hair J. , Hult, Ringle, & Sarstedt, 2022).

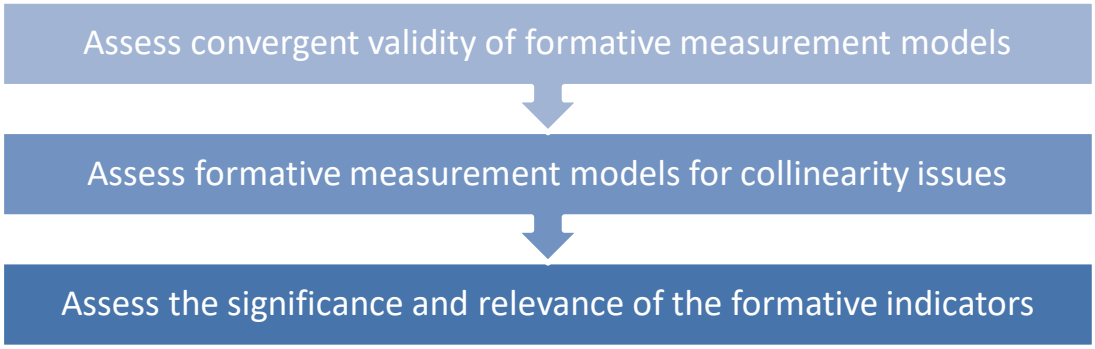

Figure 5 – Assessing formative PLS SEM reliability and validity

3.5 Possible limitations and challenges of the study

The primary challenge encountered was around encouraging participation in the study. For example, the LinkedIn post inviting participation received more than 5,000 impressions (views) but only approximately 50 actual completions.

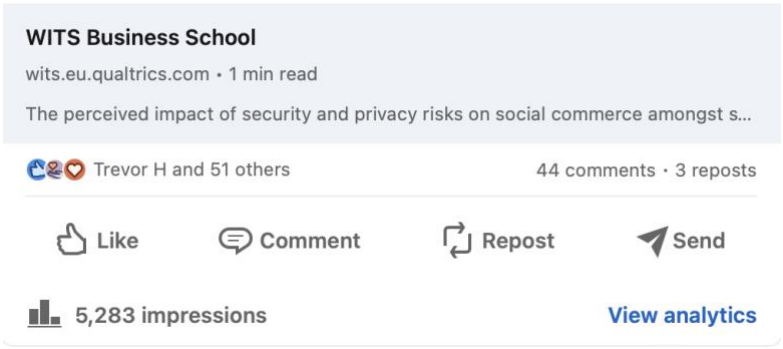

Figure 6 - LinkedIn impressions

The low participation rate could have been a result of viewers being skeptical of the authenticity of the request, not having the time to complete the survey or general disinterest/lack of incentive to do so.

Another challenge was around the use of the Smart PLS software to analyse the data, which required time to understand and learn in order to actually analyse the data. Most of the text and supporting information is written with the assumption that the reader is at an advanced or expert statistician which made for a sharp learning curve.

The low sample size, while sufficient for this analysis, means that the research results might not be generalisable to a larger sample size, or samples from other social media platforms in use in South Africa.

3.6 Ethical considerations

Given the concerns for personal safety driven by the COVID-19 pandemic and subsequent measures to limit physical contact, this study was completely virtual and made use of online survey tools to conduct data gathering.

In addition to the Wits ethics guidelines, the sample group did not supply personally identifiable information and participation was on a voluntary basis. Additionally, all respondents were adults, over the age of 18, hence the survey did not reach minors. Data from the survey is stored on the WITS Qualtrics and will be deleted once the research paper is accepted by the University.

CHAPTER 4. PRESENTATION OF RESULTS

4.1 Introduction

This section presents and describes the data ingestion process, model evaluation and the results of the PLS SEM calculations. This is followed by a discussion of the results and their implication on the research hypotheses, listed below:

H1: social media attitude positively influences social commerce intention.

H2: social media attitude positively influences social media trust.

H3: social media trust positively influences social commerce intention.

H4: the relationship between social media trust and social commerce intention is moderated by cyber security risk awareness.

H5: the relationship between social media trust and social commerce intention is moderated by privacy risk awareness.

4.2 Decriptive Statistics

This section presents the demographic information of the respondent group.

4.2.1 *Respondent Age*

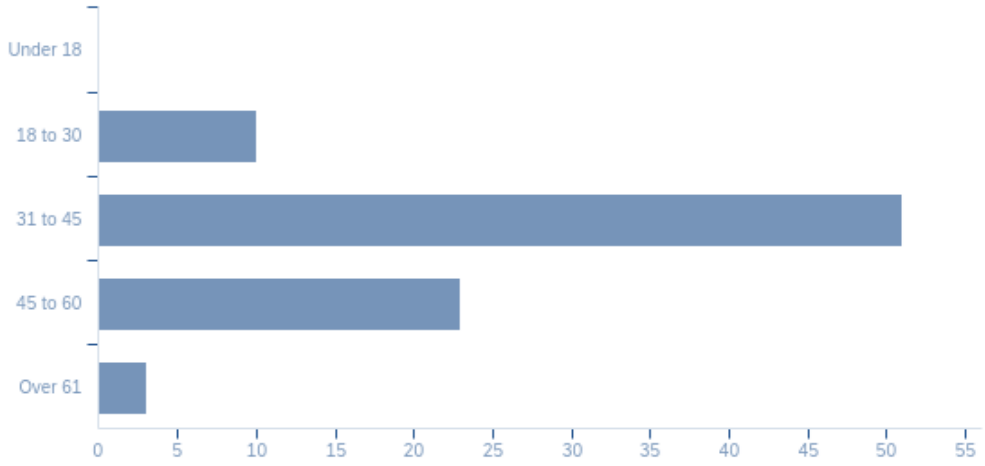

Figure 7 - Respondent Age Information

#	Answer	%	Count
1	Under 18	0.00%	0
2	18 to 30	11.49%	10
3	31 to 45	58.62%	51
4	45 to 60	26.44%	23
5	Over 61	3.45%	3
	Total	100%	87

Table 1 - Respondent Age Information

From Figure 7 and Table 1, the majority of respondents were in the 31 to 45 age group followed closely by the 45 to 60 age group. This aligns to the profile of the LinkedIn network who provided the vast majority of the survey responses.

4.2.2 *Respondent Gender*

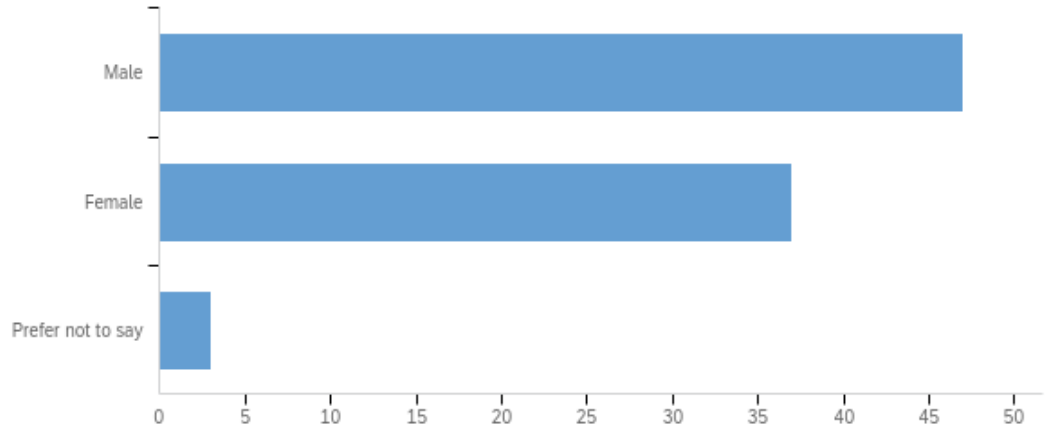

Figure 8 - Respondent Gender Information

#	Answer	%	Count
1	Male	54.02%	47
2	Female	42.53%	37
3	Non-binary / third gender	0.00%	0
4	Prefer not to say	3.45%	3
	Total	100%	87

Table 2 - Respondent Gender Information

Male and female respondents were fairly evenly represented amongst the survey respondents with male responders in the majority.

4.2.3 *Respondent education level*

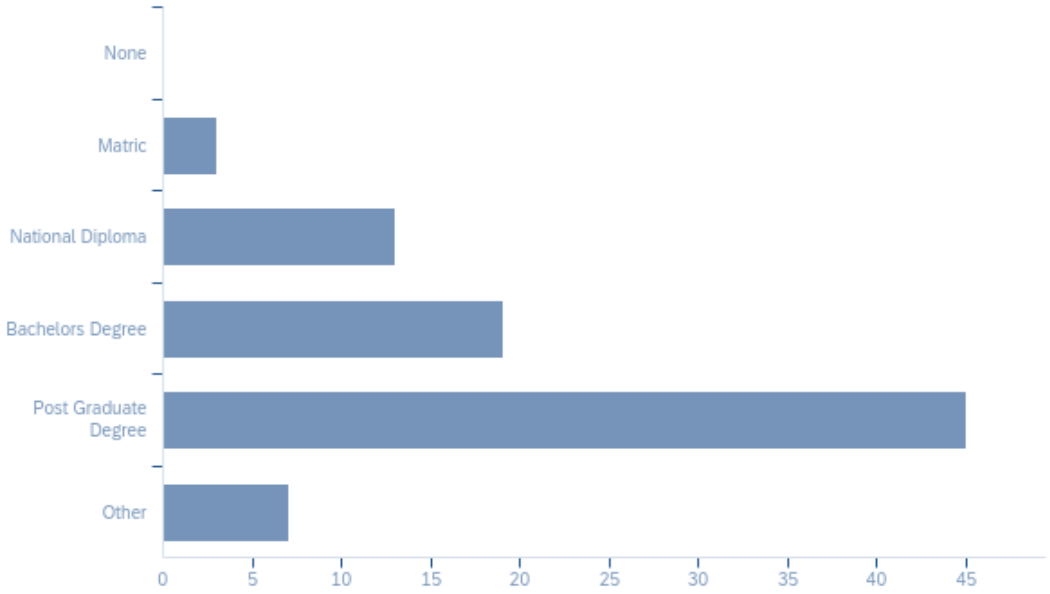

Figure 9 - Respondent education level

#	Answer	%	Count
1	None	0.00%	0
2	Matric	3.45%	3
3	National Diploma	14.94%	13
4	Bachelor's Degree	21.84%	19
5	Post Graduate Degree	51.72%	45
6	Other	8.05%	7
	Total	100%	87

Table 3 - Respondent education level

The majority of respondents held tertiary level qualifications with majority having completed post graduate studies.

4.2.4 *Respondent social media platform usage*

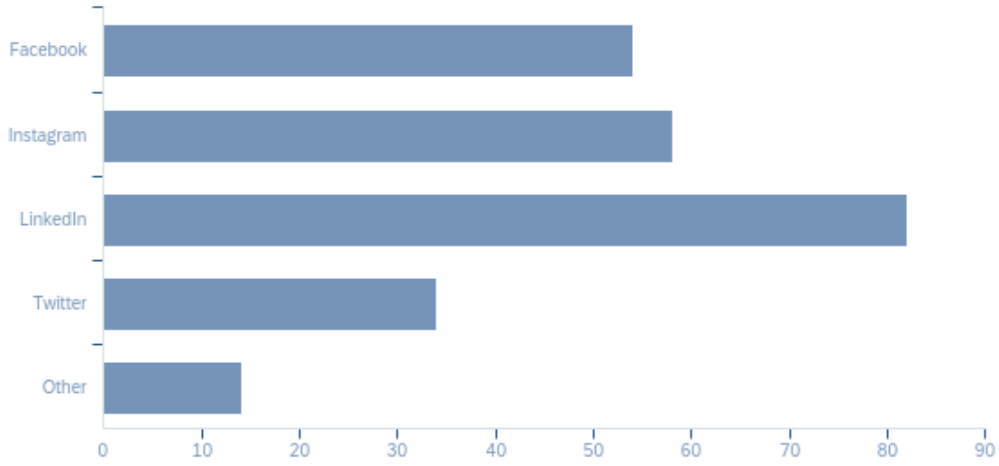

Figure 10 - Respondent social media platform usage

#	Answer	%	Count
1	Facebook	22.31%	54
2	Instagram	23.97%	58
3	LinkedIn	33.88%	82
4	Twitter	14.05%	34
5	Other	5.79%	14
	Total	100%	242

Table 4 - Social media platform usage

For the choices presented in the survey, Facebook, Instagram and LinkedIn are the most popular with Twitter and “Other” trailing by a significant margin amongst the sample group. Respondents were able to select multiple options, hence the total count of 242 responses from the 87 respondents.

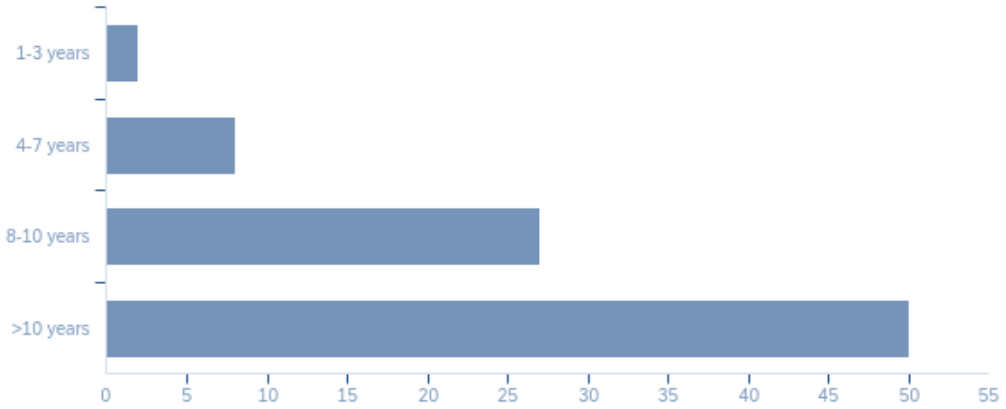

Figure 11 - Social media usage length

#	Answer	%	Count
1	1-3 years	2.30%	2
2	4-7 years	9.20%	8
3	8-10 years	31.03%	27
4	>10 years	57.47%	50
	Total	100%	87

Table 5 - Social media usage length

Corresponding to the age demographic, the majority of survey respondents had been using social media for more than 10 years. This experience was seen a positive since these respondents would have significant experience with social media platforms as these evolved over the last decade.

4.2.5 *Respondent citizenship*

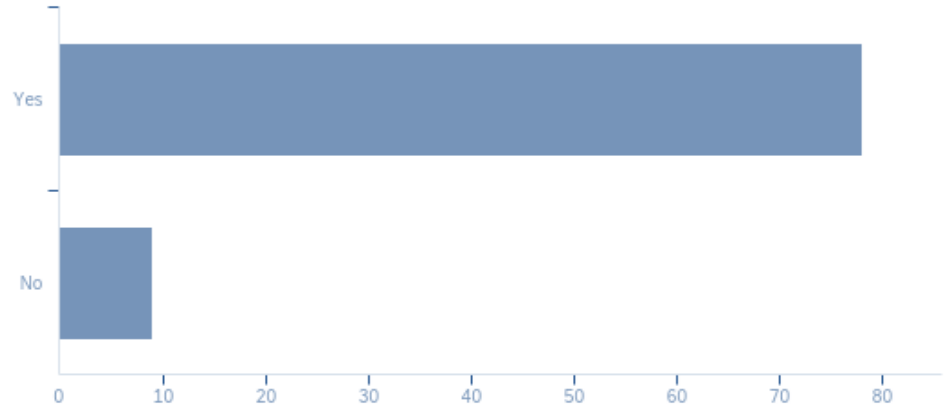

Figure 12 - Respondent citizenship

#	Answer	%	Count
1	Yes	89.66%	78
2	No	10.34%	9
	Total	100%	87

Table 6 - Respondent citizenship

The majority of respondents were South African (SA) citizens. The sample size of non-SA citizens was too small for statistical analysis to compare and contrast against the SA results and were filtered out of the dataset.

4.3 About the Smart PLS software

Modeling of the conceptual model, analysis and calculations were produced using the Smart PLS software package available at www.smartpls.com. This software package incorporates a graphical user interface to facilitate the analysis process and is available with both Student (free) and Professional licences (paid). This research and analysis was conducted using the Student version.

4.4 Data formatting for use in Smart PLS

The raw survey data from Qualtrics was “cleaned” to conform to the Smart PLS data import requirements. This cleaning entailed:

1. Exporting the Qualtrics data to Microsoft Excel as a .XLSX file in order to filter out non-South African respondent data.
2. Deleting unneeded meta data from the Qualtrics report to focus only on the primary data set.
3. This data set was then saved as a .CSV file, which was imported into Smart PLS.
4. All fields were set to “Metric” in the Smart PLS software to allow usage in the conceptual model build in Smart PLS.

The research conceptual model produced the following formative Smart PLS framework (shown with indicators hidden), with Social Media Attitude, Social Media Trust, Social Commerce Intention, Security Risk Awareness and Privacy Risk Awareness as endogenous variables. Age, Gender, Online Shopping Experience, Education Level, and Social Media (Usage) as control variables. The solid lines indicate direct relationships, while the dashed lines indicate the moderating relationships to be assessed. These relationships are labelled corresponding to the Hypothesis being tested for convenience.

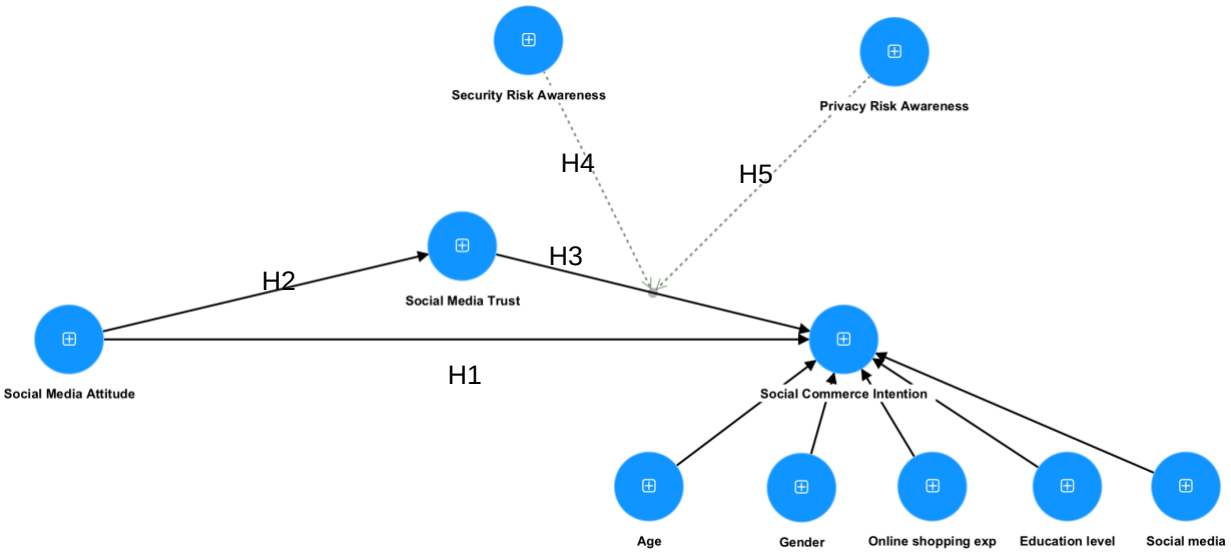

Figure 13 - Smart PLS model depicting endogenous variables, control variables and their relationships

The figure below depicts the full model with indicators visible.

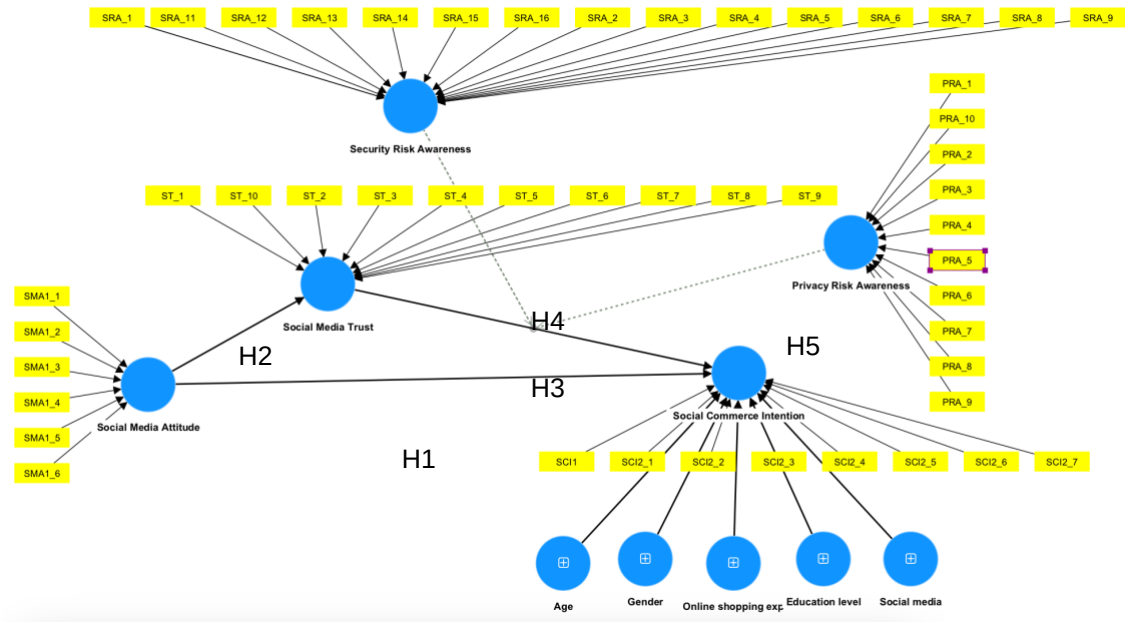

Figure 14 - PLS SEM model with key indicators visible

Evaluation of the PLS SEM result follows a two stage process (Hair J. , Hult, Ringle, & Sarstedt, 2022). First, the measurement model (outer model) is assessed for reliability and validity, and then the structural model is evaluated to

determine the statistical significance of the indicators and their relationships to draw conclusions on hypothesis validity (Hair, Risher, Sarstedt, & Ringle, 2018). The SmartPLS software supports the evaluation of the measurement & structural model in the same interface.

4.5 Phase 1 – Measurement Model Assessment

The first stage in assess a formative PLS SEM model requires the following steps:

1. Assess the model for collinearity issues (Variation Inflation Factor (VIF)),
2. Assess the significance and relevance of the formative indicators.

These factors were assessed according to the following thresholds (Hair, Risher, Sarstedt, & Ringle, 2018):

Element	Threshold
Collinearity (VIF)	• Critical collinearity issues when VIF >= 5 • Possible collinearity issues when VIF is between 3 and 5 • Ideally show that VIF < 3
Statistical significance of weights	• p-value < 0.05 (95% confidence interval or BCa not equal to 0
Relevance of indicators with a significant weight	• Larger significant weights contribute more

Relevance of indicators with a non-significant weight	• Loadings of >=0.50 that are statistically significant are considered relevant

Table 7 - Element thresholds in formative model evaluation

4.5.1 *Multicollinearity assessment*

Initial calculation of the produced the following Variance Inflation Factor (VIF) for the outer model.

Indicator	VIF
Education level	1.000
Gender	1.000
Online shopping exp	1.000
PRA_1	1.762
PRA_10	2.358
PRA_2	1.408
PRA_3	2.275
PRA_4	1.227
PRA_5	3.109
PRA_6	2.855
PRA_7	1.884
PRA_8	1.754
PRA_9	1.471
SCI1	1.366
SCI2_1	2.108
SCI2_2	2.642
SCI2_3	1.923
SCI2_4	1.543
SCI2_5	1.300
SCI2_6	1.389
SCI2_7	1.431
SMA1_1	1.994
SMA1_2	1.828
SMA1_3	2.095
SMA1_4	1.719

SMA1_5	2.770
SMA1_6	2.245
SRA_1	1.794
SRA_10	1.426
SRA_11	1.179
SRA_12	1.342
SRA_13	1.482
SRA_14	1.709
SRA_15	2.600
SRA_16	2.658
SRA_2	1.860
SRA_3	1.793
SRA_4	1.787
SRA_5	1.246
SRA_6	1.826
SRA_7	1.692
SRA_8	1.510
SRA_9	1.416
ST_1	1.713
ST_10	2.837
ST_2	5.002
ST_3	5.656
ST_4	1.310
ST_5	1.447
ST_6	2.576
ST_7	2.060
ST_8	1.470
ST_9	2.799
Social media	1.000
Age	1.000
Security Risk Awareness x Social Media Trust	1.000
Privacy Risk Awareness x Social Media Trust	1.000

The initial result indicated that ST_2 and ST_3 were beyond the collinearity threshold. The next step was to assess the loading and weighting in the model to determine their significance in the overall score. This examination revealed the ST_3=-0.389 and ST_4=0.305, which meant that these were significant factors in the overall score and were thus maintained in the model. In order to mitigate the collinearity effect, both ST_2 & ST_3 were combined into single higher order

construct (Hair Jr, et al., 2021). The model was then recalculated to asses VIF, and produce the results in the table below.

Indicator	VIF
Education level	1.000
Gender	1.000
Online shopping exp	1.000
PRA_1	1.762
PRA_10	2.358
PRA_2	1.408
PRA_3	2.275
PRA_4	1.227
PRA_5	3.109
PRA_6	2.855
PRA_7	1.884
PRA_8	1.754
PRA_9	1.471
SCI1	1.366
SCI2_1	2.108
SCI2_2	2.642
SCI2_3	1.923
SCI2_4	1.543
SCI2_5	1.300
SCI2_6	1.389
SCI2_7	1.431
SMA1_1	1.994
SMA1_2	1.828
SMA1_3	2.095
SMA1_4	1.719
SMA1_5	2.770
SMA1_6	2.245
SRA_1	1.794
SRA_10	1.426
SRA_11	1.179
SRA_12	1.342
SRA_13	1.482
SRA_14	1.709
SRA_15	2.600
SRA_16	2.658
SRA_2	1.860

SRA_3	1.793
SRA_4	1.787
SRA_5	1.246
SRA_6	1.826
SRA_7	1.692
SRA_8	1.510
SRA_9	1.416
ST_1	1.243
ST_10	2.574
ST_2	4.154
ST_3	4.154
ST_4	1.168
ST_5	1.445
ST_6	2.395
ST_7	2.050
ST_8	1.465
ST_9	2.722
Social media	1.000
Age	1.000
Security Risk Awareness x Social Media Trust	1.000
Privacy Risk Awareness x Social Media Trust	1.000

The combined indicators produced VIF scores below 5, meaning that these now met the threshold requirements, with the multicollinearity effect being adequately mitigated.

4.5.2 *Significance and relevance of the formative indicators*

The magnitude and signs of the weights were assessed to determine the significance and relevance of the outer model indicators. The weights alone do not provide information about their statistical significance, which requires the calculation of the t-value and p-values from the bootstrapped model (Hair J. , Hult, Ringle, & Sarstedt, 2022).

The qualitative evaluation of the weights based on their magnitudes and sign produced the following results. (Hair Jr, et al., 2021)

High weights (absolute value > 0.5):

- PRA_2: -0.527
- PRA_6: 0.533
- PRA_7: -0.547
- SMA1_6: 0.647
- SRA_9: 0.664
- ST_1: 0.501

These indicators have a strong contribution to their respective latent variables and are likely to be relevant in the model (Hair, Matthews, Matthews, & Sarstedt, 2017).

Moderate weights (absolute value between 0.3 and 0.5):

- PRA_1: -0.296
- PRA_4: 0.350
- SCI1: 0.427
- SCI2_3: 0.326
- SCI2_6: 0.334
- SMA1_2: 0.312
- SMA1_5: 0.269
- SRA_3: 0.332
- SRA_5: 0.315
- ST_2: 0.305
- ST_3: -0.389
- ST_4: 0.305
- ST_6: 0.363
- ST_8: 0.324

These indicators have a moderate contribution to their respective latent variables and means they are relevant in the model (Hair, Matthews, Matthews, & Sarstedt, 2017)

Low weights (absolute value < 0.3):

The remaining indicators have low weights, suggesting a weak contribution to their respective latent variables. Further analysis was deferred to the bootstrap anlaysis of the model.

Bootstrapping of the model with 10,000 samples produced the following p-values for the indicator outer weights and loadings.

	Outer loadings P values	Outer weights P values
Education level <- Education level	0.000	0.000
Gender <- Gender	0.000	0.000
Online shopping exp <- Online shopping exp	0.000	0.000
PRA_1 -> Privacy Risk Awareness	0.634	0.417
PRA_10 -> Privacy Risk Awareness	0.748	0.522
PRA_2 -> Privacy Risk Awareness	0.255	0.310
PRA_3 -> Privacy Risk Awareness	0.557	0.682
PRA_4 -> Privacy Risk Awareness	0.330	0.292
PRA_5 -> Privacy Risk Awareness	0.188	0.526
PRA_6 -> Privacy Risk Awareness	0.186	0.351
PRA_7 -> Privacy Risk Awareness	0.523	0.226
PRA_8 -> Privacy Risk Awareness	0.984	0.616
PRA_9 -> Privacy Risk Awareness	0.419	0.438
SCI1 -> Social Commerce Intention	0.000	0.033
SCI2_1 -> Social Commerce Intention	0.000	0.895
SCI2_2 -> Social Commerce Intention	0.000	0.622
SCI2_3 -> Social Commerce Intention	0.000	0.298
SCI2_4 -> Social Commerce Intention	0.002	0.666
SCI2_5 -> Social Commerce Intention	0.326	0.449
SCI2_6 -> Social Commerce Intention	0.000	0.041
SCI2_7 -> Social Commerce Intention	0.001	0.294
SMA1_1 -> Social Media Attitude	0.000	0.498
SMA1_2 -> Social Media Attitude	0.000	0.146
SMA1_3 -> Social Media Attitude	0.000	0.420
SMA1_4 -> Social Media Attitude	0.019	0.548
SMA1_5 -> Social Media Attitude	0.000	0.237
SMA1_6 -> Social Media Attitude	0.000	0.007
SRA_1 -> Security Risk Awareness	0.296	0.692
SRA_10 -> Security Risk Awareness	0.510	0.746
SRA_11 -> Security Risk Awareness	0.775	0.403

SRA_12 -> Security Risk Awareness	0.772	0.990
SRA_13 -> Security Risk Awareness	0.503	0.760
SRA_14 -> Security Risk Awareness	0.257	0.288
SRA_15 -> Security Risk Awareness	0.587	0.891
SRA_16 -> Security Risk Awareness	0.760	0.978
SRA_2 -> Security Risk Awareness	0.236	0.620
SRA_3 -> Security Risk Awareness	0.364	0.252
SRA_4 -> Security Risk Awareness	0.947	0.388
SRA_5 -> Security Risk Awareness	0.157	0.222
SRA_6 -> Security Risk Awareness	0.673	0.437
SRA_7 -> Security Risk Awareness	0.171	0.554
SRA_8 -> Security Risk Awareness	0.228	0.218
SRA_9 -> Security Risk Awareness	0.144	0.143
ST_1 -> Social Media Trust	0.000	0.000
ST_10 -> Social Media Trust	0.003	0.597
ST_2 -> Combined	0.000	0.663
ST_3 -> Combined	0.000	0.321
ST_4 -> Social Media Trust	0.001	0.042
ST_5 -> Social Media Trust	0.055	0.439
ST_6 -> Social Media Trust	0.000	0.293
ST_7 -> Social Media Trust	0.000	0.903
ST_8 -> Social Media Trust	0.001	0.093
ST_9 -> Social Media Trust	0.000	0.637
Social media <- Social media	0.000	0.000
Age <- Age	0.000	0.000
Privacy Risk Awareness x Social Media Trust -> Privacy Risk Awareness x Social Media Trust	0.000	0.000
Security Risk Awareness x Social Media Trust -> Security Risk Awareness x Social Media Trust	0.000	0.000

Table 8 - Outer weights and loadings p-value data

4.6 Phase 2 – Structural Model Assessment

The second phase of evaluating the PLS SEM entailed evaluating the structural model using the PLS SEM bootstrap procedure.

4.6.1 *Structural Model Assessment Criteria*

The following criteria were assessed to validate the PLS SEM structural model:

1. Coefficient of Determination (R^2): R^2 measures the proportion of variance in the dependent variables that can be explained by the independent variables. R^2 values range from 0 to 1. Higher R^2 values indicate better explanatory power. For this evaluation, R^2 values of 0.25, 0.50, and 0.75 were considered weak, moderate, and substantial, respectively (Hair, Risher, Sarstedt, & Ringle, 2018).

2. Path Coefficients: Path coefficients represent the strength and direction of the relationship between variables in the model. Analysis of the path coefficients' magnitude and significance determined the importance of relationships amongst constructs. A significant path coefficient ($p < 0.05$) implied a substantial relationship between the constructs.

3. Effect Sizes (f^2): Analysis of the f^2 value was used to measure the impact of the independent variables on the dependent variables, considering other independent variables in the model. For this analysis, f^2 values of 0.02, 0.15, and 0.35 were considered small, medium, and large effects, respectively (Cohen, 1988)

4. Collinearity Assessment: Multicollinearity (VIF) was evaluated amongst the predictor variables to ensure that they did not have a high degree of multicollinearity. A VIF value below 5 was considered acceptable (Hair, Matthews, Matthews, & Sarstedt, 2017)

5. Predictive Relevance (Q^2): The Q^2 value measured the model's predictive accuracy using the blindfolding procedure. Q^2 values greater than zero indicated that the model had predictive relevance (Hair, Hult, & Ringle, A primer on partial least squares structural equation modeling (PLS-SEM), 2016).

6. Discriminant Validity, which is the measure of the extent to which a construct is empirically distinct from other constructs in the model. Measuring Discriminant Validity establishes that constructs are capturing distinct results, not represented by other constructs in the model (Hair, Hult, & Ringle, A primer on partial least squares structural equation modeling (PLS-SEM), 2016) (Hair Jr, et al., 2021).

4.6.2 *Structural Model Assessment Results*

a. *R^2 Results*

The PLS SEM model contains two endogenous (dependent) variables, namely Social Commerce Intention and Social Media Trust which produce the following R^2 result:

Indicator	R-square
Social Commerce Intention	0.647
Social Media Trust	0.528

Table 9 - R^2 Results

b. *Path Coefficients*

The table below displays the results of the path coefficient analysis from the boostrapped model (using 10,000 samples).

Relationship	Original sample (O)	T statistics (|O/STDEV|)	P values
Age -> Social Commerce Intention	-0.156	1.287	0.099
Combined -> Social Media Trust	0.327	2.474	0.007
Education level -> Social Commerce Intention	-0.094	0.913	0.181
Gender -> Social Commerce Intention	0.119	1.291	0.098
Online shopping exp -> Social Commerce Intention	-0.042	0.424	0.336
Privacy Risk Awareness -> Social Commerce Intention	0.099	0.540	0.294

Security Risk Awareness -> Social Commerce Intention	0.407	0.991	0.161
Social Media Attitude -> Social Commerce Intention	-0.031	0.176	0.430
Social Media Attitude -> Social Media Trust	0.576	5.723	0.000
Social Media Exp -> Social Commerce Intention	-0.036	0.344	0.365
Social Media Trust -> Social Commerce Intention	0.447	2.102	0.018
Privacy Risk Awareness x Social Media Trust -> Social Commerce Intention	-0.009	0.091	0.464
Security Risk Awareness x Social Media Trust -> Social Commerce Intention	-0.046	0.460	0.323

Table 10 - Path coefficient results

The figures below depict the Simple Slopes analysis used to examine the effect of the moderating variables, namely, Security Risk Awareness and Privacy Risk Awareness.

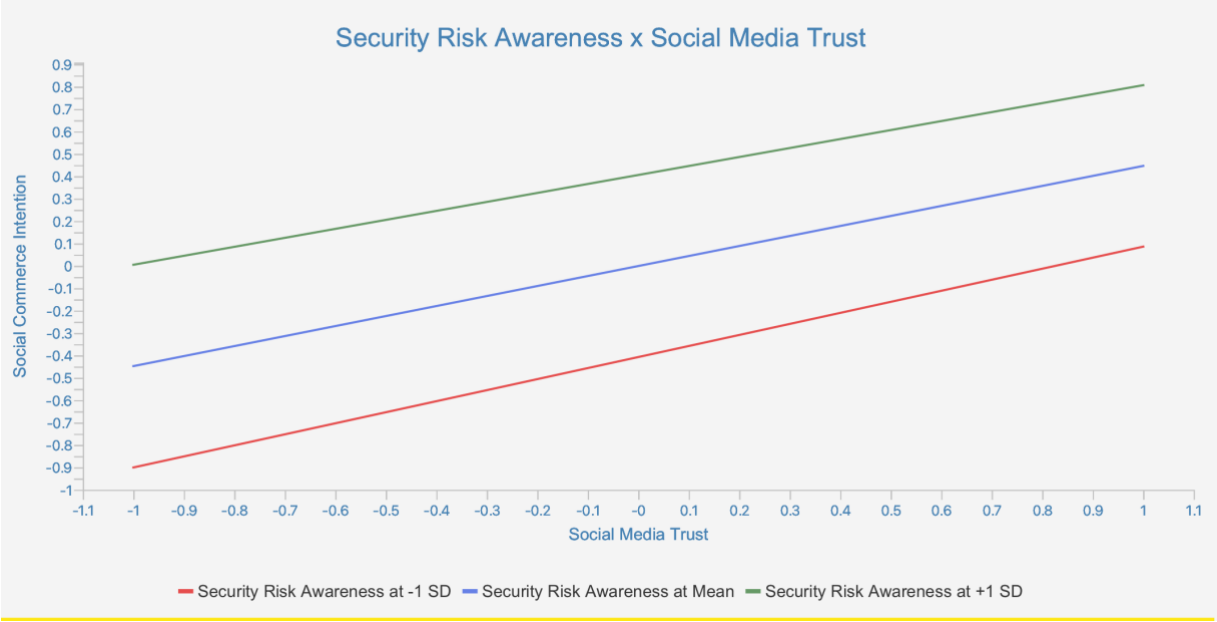

Figure 15 - Effect of Security Risk Awareness as a moderating variable

The green and red lines in figure 17 represent the relationship between Security Risk Awareness for low and high levels of the moderator construct with Social Media Trust. The nearly parallel slopes indicate that for this sample group, Security Risk Awareness is a weak moderator of Social Media Trust (Hair Jr, et al., 2021).

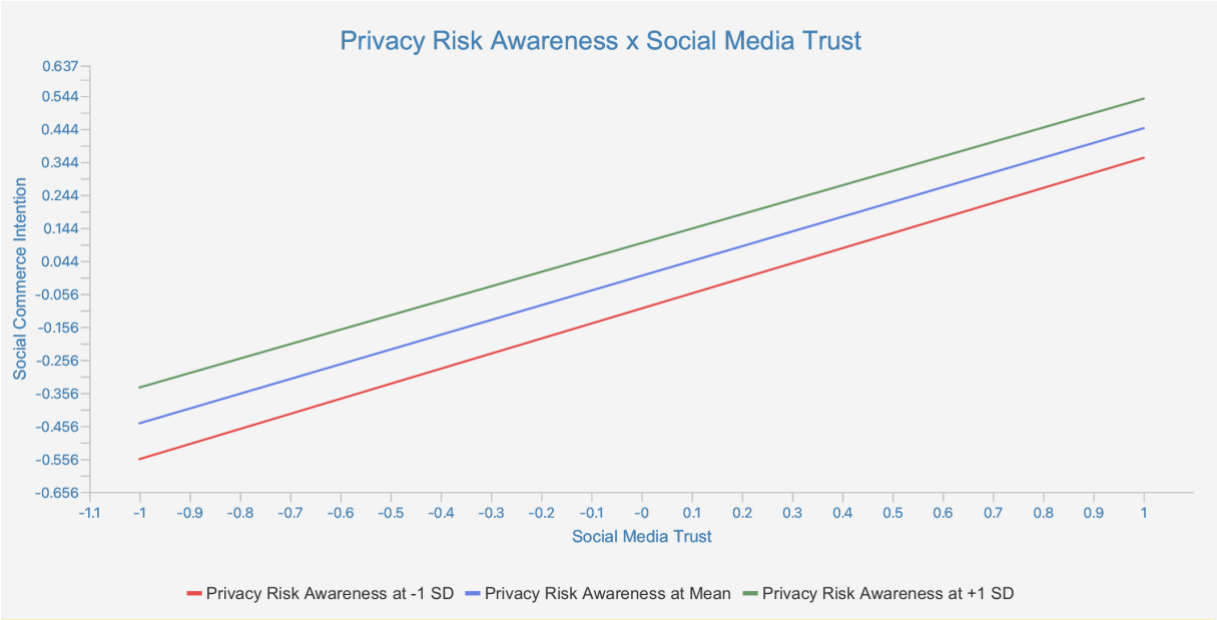

Figure 16 - Effect of Privacy Risk Awareness as a moderating variable

The analysis in figure 18 shows that, for this sample group, Privacy Risk Awareness is a weak moderating factor on Social Commerce intention, at best (Hair Jr, et al., 2021). This implies that the sample group are either pre-selecting platforms through an alternative channel, e.g. word of mouth or forums and then engaging in social commerce on recommended sites, or that the sample group trusted their social commerce sites implicitly.

c. *Effect Sizes (f^2)*

The table below shows the result of the f^2 calculation per the affected construct/s.

	Social Commerce Intention	Social Media Trust
Age	0.039	
Combined		0.250

Education level	0.029	
Gender	0.024	
Online shopping exp	0.008	
Privacy Risk Awareness	0.006	
Security Risk Awareness	0.198	
Social Commerce Intention		
Social Media Attitude	0.000	0.640
Social Media Exp	0.006	
Social Media Trust	0.213	
Privacy Risk Awareness x Social Media Trust	0.000	
Security Risk Awareness x Social Media Trust	0.002	

Table 11 - Effect sizes calculation results

d. *Collinearity Assessment*

The VIF assessment of the outer structural are displayed in the table below.

Outer model

Indicator	VIF
Education level	1.000
Gender	1.000
Online shopping exp	1.000
PRA_1	1.762
PRA_10	2.358
PRA_2	1.408
PRA_3	2.275
PRA_4	1.227
PRA_5	3.109
PRA_6	2.855
PRA_7	1.884
PRA_8	1.754
PRA_9	1.471
SCI2_1	1.892
SCI2_2	2.678
SCI2_3	2.023
SCI2_4	1.688
SCI2_6	1.383
SCI2_7	1.422
SMA1_1	1.994

SMA1_2	1.828
SMA1_3	2.095
SMA1_4	1.719
SMA1_5	2.770
SMA1_6	2.245
SRA_1	1.794
SRA_10	1.426
SRA_11	1.179
SRA_12	1.342
SRA_13	1.482
SRA_14	1.709
SRA_15	2.600
SRA_16	2.658
SRA_2	1.860
SRA_3	1.793
SRA_4	1.787
SRA_5	1.246
SRA_6	1.826
SRA_7	1.692
SRA_8	1.510
SRA_9	1.416
ST_1	1.243
ST_10	2.574
ST_2	4.154
ST_3	4.154
ST_4	1.168
ST_5	1.445
ST_6	2.395
ST_7	2.050
ST_8	1.465
ST_9	2.722
Age	1.425
Age	1.000
Security Risk Awareness x Social Media Trust	1.000
Privacy Risk Awareness x Social Media Trust	1.000

Table 12 - Outer Model VIF Results

e. *Predictive Relevance (Q2) Results*

Predictive relevance (Q^2) is a statistical measure in use do to assess the structural model's predictive accuracy of the PLS SEM model's constructs. The Q^2 value was calculated using the PLSpredict algorithm within the SmartPLS software. PLSpredict implements a Blindfolding (cross-validation) procedure (Hair, Sarstedt, Ringle, & Gudergan, 2017).

A $Q^2>0$ indicates positive predictive relevance, and higher the Q^2, the greater the predictive relevance on the endogenous variables. The table below displays the results of the Q^2 calculation.

Endogenous Variable	Q^2predict
Social Commerce Intention	0,027
Social Media Trust	0,253

Table 13 - Results of the Q2 calculation

f. *Discriminant Validity*

The discriminant validity was assessing using heterotrait-monotrait ratio (HTMT), which is the ratio of the between-trait to within-trait correlations. (Henseler, 2016) suggests a threshold value of 0.90 if path constructs are similar and a threshold value of 0.85 if the paths are conceptually more distinct. Results above these thresholds indicate that the constructs lack discriminant validity. The table below shows the results of the HTMT analysis and indicates high discriminant validity between the constructs.

	Original sample (O)	Sample mean (M)	2.5%	97.5%
Education level <-> Age	0.148	0.154	0.009	0.331
Gender <-> Age	0.055	0.089	0.004	0.244
Gender <-> Education level	0.056	0.090	0.003	0.237

Online shopping exp <-> Age	0.028	0.140	0.005	0.372
Online shopping exp <-> Education level	0.009	0.107	0.004	0.298
Online shopping exp <-> Gender	0.049	0.109	0.004	0.292
Social media <-> Age	0.021	0.110	0.004	0.305
Social media <-> Education level	0.068	0.096	0.004	0.224
Social media <-> Gender	0.030	0.082	0.003	0.229
Social media <-> Online shopping exp	0.109	0.131	0.006	0.308

Table 14 - HTMT Results

4.7 Results of the PLS SEM Analysis

The direction and strength of the path coefficient relationships suggest the following:

1. Age on Social Commerce Intention: The path coefficient is -0.130, suggesting a negative relationship between age and social commerce intention. As age increases, social commerce intention decreases.

2. Combined on Social Media Trust: The path coefficient is 0.352, indicating a positive relationship between the combined construct and social media trust. As the combined construct increases, social media trust increases as well.

3. Education level on Social Commerce Intention: The path coefficient is -0.110, implying a negative relationship between education level and social commerce intention. As the education level increases, social commerce intention decreases.

4. Gender on Social Commerce Intention: The path coefficient is 0.108, suggesting a positive relationship between gender and social commerce

intention. This indicates that there might be gender differences in social commerce intention.

5. Online shopping experience on Social Commerce Intention: The path coefficient is -0.055, indicating a negative relationship between online shopping experience and social commerce intention. As the online shopping experience increases, social commerce intention decreases.

6. Privacy Risk Awareness on Social Commerce Intention: The path coefficient is 0.060, suggesting a weak positive relationship between privacy risk awareness and social commerce intention. As privacy risk awareness increases, social commerce intention slightly increases.

7. Security Risk Awareness on Social Commerce Intention: The path coefficient is 0.424, indicating a strong positive relationship between security risk awareness and social commerce intention. As security risk awareness increases, social commerce intention increases.

8. Social Media Attitude on Social Commerce Intention: The path coefficient is 0.007, which is very close to zero, suggesting no or very weak relationship between social media attitude and social commerce intention.

9. Social Media Attitude on Social Media Trust: The path coefficient is 0.563, indicating a strong positive relationship between social media attitude and social media trust. As social media attitude increases, social media trust increases as well.

10. Social Media Exp on Social Commerce Intention: The path coefficient is -0.051, suggesting a weak negative relationship between social media experience and social commerce intention. As social media experience increases, social commerce intention slightly decreases.

11. Social Media Trust on Social Commerce Intention: The path coefficient is 0.407, indicating a strong positive relationship between social media trust

and social commerce intention. As social media trust increases, social commerce intention increases.

12. Privacy Risk Awareness & Social Media Trust on Social Commerce Intention: The path coefficient is -0.009, suggesting a weak negative relationship between the interaction of privacy risk awareness and social media trust on social commerce intention.

13. Security Risk Awareness & Social Media Trust on Social Commerce Intention: The path coefficient is -0.043, suggesting a weak negative relationship between the interaction of security risk awareness and social media trust on social commerce intention.

The PLS-SEM results show strong positive relationships between security risk awareness, social media attitude, and social media trust on social commerce intention. The results also reveal negative or weak relationships between other constructs and social commerce intention. The interaction effects of privacy risk awareness x social media trust and security risk awareness x social media trust on social commerce intention are weak and negative.

The path coefficient and p-value data produced the following results for each hypothesis.

H1: Social media attitude positively influences social commerce intention.

- The path coefficient for the relationship between Social Media Attitude and Social Commerce Intention is 0.007 with a p-value of 0.475. Since the p-value is greater than the common significance level (0.05), H1 is not supported.

H2: Social media attitude positively influences social media trust.

- The path coefficient for the relationship between Social Media Attitude and Social Media Trust is 0.563 with a p-value of 0.000. Since the p-value is less than 0.05, H2 is supported.

H3: Social media trust positively influences social commerce intention.

- The path coefficient for the relationship between Social Media Trust and Social Commerce Intention is 0.407 with a p-value of 0.001. Since the p-value is less than 0.05, H3 is supported.

H4: The relationship between social media trust and social commerce intention is moderated by cyber security risk awareness.

- The path coefficient for the interaction between Security Risk Awareness x Social Media Trust and Social Commerce Intention is -0.043 with a p-value of 0.343. Since the p-value is greater than 0.05, H4 is not supported.

H5: The relationship between social media trust and social commerce intention is moderated by privacy risk awareness.

- The path coefficient for the interaction between Privacy Risk Awareness x Social Media Trust and Social Commerce Intention is -0.009 with a p-value of 0.470. Since the p-value is greater than 0.05, H5 is not supported.

These results are summarised in the table below:

Hypothesis	Statement	Result
H1	Social media attitude positively influences social commerce intention.	Not supported
H2	Social media attitude positively influences social media trust.	Supported
H3	Social media trust positively influences social commerce intention.	Supported

H4	The relationship between social media trust and social commerce intention is moderated by cyber security risk awareness.	Not supported
H5	The relationship between social media trust and social commerce intention is moderated by privacy risk awareness.	Not supported

Table 15 - Summary of PLS SEM results

4.8 Summary of the results/findings

This chapter presented and described the data ingestion process, PLS SEM model evaluation and the results of the PLS SEM calculations. This was followed by a presentation of the SEM results on the research relationships and the research hypotheses.

CHAPTER 5. DISCUSSION OF THE RESULTS OR FINDINGS

5.1 Introduction

This chapter discusses the significance of findings from Chapter 4 in relation to prior research on social commerce. The chapter structure will focus on each hypothesis in turn and then provide a chapter summary at the end.

5.2 Discussion pertaining to Hypothesis 1

The finding that social media attitude does not positively influence social commerce intention is contrary to prior research which suggests a positive relationship between these constructs (Hajli, 2012). Changing consumer behavior, the demographic surveyed, the evolving nature of social media platforms, and an increased awareness of the potential security and privacy risks involved in social commerce could explain this finding. While individuals might have positive attitudes towards social media, these attitudes alone are insufficient to drive their intent to engage in social commerce. This highlights the complexity of social commerce behavior and indicates that more research is required to understand this unexpected result.

5.3 Discussion pertaining to Hypothesis 2

The result of H2, which found that social media attitude positively influences social media trust, aligns with the previous literature (Lu, Fan, & Zhou, 2016). This result highlights the need for social media platforms to foster and maintain a positive user experience amongst use, as this will drive trust. Trust, in turn, plays a crucia role in influencing users' intention to engage in social commerce, as supported by H3.

5.4 Discussion pertaining to Hypothesis 3

The results of H3 aligns with existing research that supports the significance and importance of trust in influencing social commerce intention (Zhou, Lu, & Wang, 2013). Trust in social media platforms can reduce perceived risk and uncertainty, thereby facilitating users' willingness to participate in social commerce.

5.5 Discussion pertaining to Hypothesis 4 and 5

The results of H4 and H5, contradicts previous studies that supported the moderating effects of cybersecurity and privacy risk awareness on social media trust and social commerce intention (Krasnova, Veltri, & Günther, 2017) (Martin, Borah, & Palmatier, 2017). These findings suggest that heightened awareness of cybersecurity and privacy risks may not significantly alter the impact of social media trust on social commerce intention. This could imply that while users are aware of potential risks, their trust in the platform and the benefits of engaging in social commerce may outweigh these risks. One possible explanation could be the changing nature of users' risk perceptions and threshold, as they become more accustomed to the online environment and learn to navigate and manage these risks. Another potential explanation could be the varying impact of risk awareness on different segments of the surveyed population. Future research could explore these possibilities in more detail.

5.6 Conclusion

This chapter discussed the results of the PLS SEM results in relation to the research hypotheses and existing research.

CHAPTER 6. CONCLUSIONS & RECOMMENDATIONS

6.1 Introduction

This chapter with present conclusions per research objective and recommendations on the real-world applicability of the results. The final section of this chapter suggests areas for further research.

The research objectives, as presented in Chapter 1, were to:

1. Determine the extent to which Social Media Attitude influences social commerce intention
2. Analyse the influence of Social Media Attitude on social media trust
3. Examine the relationship between SM trust and Social Commerce Intention
4. Determine the extent to which the relationship between SM trust and SCI is moderated by cybersecurity risk awareness
5. Determine the extent to which the relationship between SM trust and SCI is moderated by privacy risk awareness

6.2 Conclusions regarding research objective 1

The research results suggest that positive or negative social media sentiment is not a strong predictor of social commerce intention. The research suggests that more complex decision making is at play, in addition to, or superceding the social media sentiment.

The findings suggest that while social media attitude may influence the acceptance of social media generally, it doesn't necessarily translate into the intention to use social media for commerce. This suggests that other factors may be more significant in shaping social commerce intention. For instance, perceived usefulness or perceived ease of use, as suggested by the Technology Acceptance Model (TAM)) could be more influential (Davis, 1989). Businesses should strive to foster positive attitudes towards their social media platforms, they

should also ensure that their social commerce features are perceived as useful, trustworthy, and easy to use.

6.3 Conclusions regarding research objective 2

The research indicated a positive and significant relationship between social media attitude and social media trust, suggesting that users who have a positive attitude towards social media are likely to trust it more.

This finding supports existing literature suggesting that users with positive attitudes towards a platform are more likely to trust it (Lu, Fan, & Zhou, 2016). Fostering positive attitudes towards a social media platform can be a viable strategy to build user trust, since trust is a critical factor in social and electronic commerce (Pavlou, 2003). For example, vendors using social commerce as a channel to market should implement authentic, high quality content, transparent privacy and security controls and respond to user queries quickly to foster a positive attitude and enhance trust (Chen & Dibb, 2010).

6.4 Conclusions regarding research objective 3

The research confirmed that trust in social media has a positive and significant influence on social commerce intention, further supporting prior research on the critical role of trust in the intention to participate in social commerce.

However, an area that this research did not address is the dynamic nature of this trust relationship, in light of data breaches and exposures. The nature of the trust relationship with each social media platform may also vary on a spectrum, which requires further examination. Trust has long been recognized as an essential prerequisite for online commerce due to the uncertainty and perceived risks inherent in the online environment (Pavlou, 2003). This indicates that trust-building should be a priority for businesses and social media platforms seeking to promote social commerce. The findings of research objective 3 reinforce those

of objective 2, further demonstrating the strong interplay between the concepts of social media trust, social media attitude and social commerce intention.

6.5 Conclusions regarding research objectives 4 and 5

The research did not support the hypothesis that cybersecurity and/or privacy risk awareness moderates the relationship between social media trust and social commerce intention. This finding is contrary to prior research which identified privacy and security concerns as critical barriers to online commerce (Li, 2014). This suggests that the surveyed group's awareness of cybersecurity and privacy risks and issues, did not significantly impact the relationship between their trust in social media and their intention to engage in social commerce, if they trust the platform.

This could mean that other factors or data were being used to moderate the strength and direction of the trust relationship. This finding suggests that trust can mitigate the potential negative impact of risk awareness on social commerce intention. However, it does not undermine the importance of maintaining strong cybersecurity measures and transparent,easy to understand privacy policies. Ensuring users' awareness that these measures are in place could further foster trust and encourage social commerce participation.

6.6 Recommendations

Some of the recommendations for businesses, marketers, and social media platforms looking to leverage social commerce include:

1. Maintain and enhance trust: The research showed that social media trust significantly impacted social commerce intention which means that businesses should focus on strategies to build and enhance trust on their platforms and social channels (Zhou, Lu, & Wang, 2013). These methods include transparent communications, e.g. data breach notifications, secure

payment systems and processes, and honest customer reviews of products and services (Kim, Ferrin, & Rao, 2008).

2. Positive User Experience: Providing a positive user experience on social media platforms is a high priority, since positive social media attitudes led to increased social media trust (Lu, Fan, & Zhou, 2016). Some of the dimensions that support a positive user experience include simple navigation across multiple form-factors and device platforms, personalised content as an opt-in feature, relevant content based on the user's preferences and prompt problem management with payments, logistics and other product or platform disputes.
3. Understandable Cybersecurity and Privacy Policies: Even though the research did not find a significant moderation effect of cybersecurity and privacy risk awareness on the relationship between social media trust and social commerce intention, these aspects are still important given the growing concern about data privacy and security amongst online users (Krasnova, Veltri, & Günther, 2017). Businesses should invest in strong data security measures and ensure their privacy policies are transparent and user-friendly.
4. User awareness: While attitudes toward social media did not directly influence social commerce intention in this study, educating users about the benefits and conveniences of social commerce could help drive adoption (Hajli, 2012). This could involve influencer campaigns, promotional offers and other engaging devices to create user awareness and adoption.

These recommendations can help businesses and social media platforms create an environment conducive to social commerce, thereby leveraging the power of social media to drive sales and engagement.

6.7 Suggestions for further research

The research results also suggest a need for further investigation into the factors that can influence the relationship between social media trust, attitudes, and social commerce intention. Additional factors, such as perceived usefulness, social influence, or demographic variables, could also be considered in future research.

Bibliography

McKinsey. (2020, October 5). *COVID-19 digital transformation and technology*. Retrieved from McKinsey : https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever

Kemp, S. (2022, February 15). *DIGITAL 2022: SOUTH AFRICA*. Retrieved from DataReportal: https://datareportal.com/reports/digital-2022-south-africa

Statista. (2022). *Number of social network users in South Africa from 2017 to 2026*. Retrieved from Statista: https://www.statista.com/statistics/972776/number-of-social-network-users-in-south-africa/

Dollarhide, M. (2022, March 27). *What is Social Commerce?* . Retrieved from Investopedia: https://www.investopedia.com/terms/s/social-commerce.asp#:~:text=and%20financial%20planning.-,What%20Is%20Social%20Commerce%3F,retweets%2C%20likes%2C%20and%20shares.

SurfShark. (2021). *Cybercrime Statistics*. Retrieved from SurfShark: https://surfshark.com/research/data-breach-impact/statistics

Kimery, K., & McCord, M. (2006). Signals of Trustworthiness in E-Commerce: Consumer Understanding of Third-Party Assurance Seals. *Journal of Electronic Commerce in Organizations*, 52-74.

Statista. (2022). *Digital population in South Africa as of January 2022*. Retrieved from Statista: https://www.statista.com/statistics/685134/south-africa-digital-population/

World Bank. (2022). *Individuals using the Internet (% of population) - South Africa*. Retrieved from World Bank: https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=ZA

Business Insider. (2020, June 3). *Hackers on the dark web love South Africa - here's why we suffer 577 attacks per hour*. Retrieved from Business Insider South Africa: https://www.businessinsider.co.za/sa-third-highest-number-of-cybercrime-victims-2020-6

ITU. (2019). *Global Cybersecurity Index 2018.* Retrieved from ITU: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Niekerk, B. v. (2017). An Analysis of Cyber-Incidents in South Africa. *The African Journal of Information and Communication*, 113-132. Retrieved from Scielo: http://www.scielo.org.za/pdf/ajic/v20/06.pdf

Sutherland, E. (2017). Governance of cybersecurity - The case of South Africa. *The African Journal of Information and Communication*, 83-112. Retrieved from http://www.scielo.org.za/scielo.php?pid=S2077-72132017000100005&script=sci_arttext&tlng=es

Gcaza, N., & Solms, R. v. (2017). A STRATEGY FOR A CYBERSECURITY CULTURE: A SOUTH AFRICAN PERSPECTIVE. *The Electronic Journal of Information Systems in Developing Countries*, 1-17.

Mabunda, S. (2021). Cybersecurity in South Africa: Towards Best Practices. *CyberBRICS*, 227-270.

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, 77-81. Retrieved from Cybercrime and Cybersecurity in Africa

Kaspersky. (2022). *What is cyber security?* . Retrieved from Kaspersky: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

ITGovernance. (2022). *What is cyber security? Definition and best practise*. Retrieved from ITGovernance: https://www.itgovernance.co.uk/what-is-cybersecurity

CISA. (2019, November 14). *What is cybersecurity? | CISA*. Retrieved from Cybersecurity and infrastructure security agency: https://www.cisa.gov/uscert/ncas/tips/ST04-001

IAPP. (2022). *What is privacy*. Retrieved from International Association of Privacy Professionals : https://iapp.org/about/what-is-privacy/

NIST. (2022). *privacy - Glossary | CRSC*. Retrieved from NIST Computer Security Resource Centre: https://csrc.nist.gov/glossary/term/privacy

Horzum, M. B. (2016). Examining the relationship to gender and personality on the purpose. *Computers in Human Behavior*, 319-328.

Ngai, E. W., Tao, S. S., & Moon, K. K. (2015). Social media research: Theories, constructs, and conceptual. *International Journal of Information Management*, 33-44.

McFarland, L. A., & Ployheart, R. E. (2015). Social Media: A conceptual framework to guide research and practice. *Journal of Applied Psychology*, 1653-1677.

DülekIbrahim, B., & aydın, I. (2020). *EFFECT OF SOCIAL MEDIA MARKETING ON E-WOM, BRAND LOYALTY, AND PURCHASE INTENT.* Bingöl Üniversitesi Sosyal Bilimler Enstitüsü Dergis.

Chow, W. S., & Shi, S. (2014). UNDERSTANDING CONSUMER TRUST IN SOCIAL COMMERCE WEBSITES. *Pacific Asia Conference on Information Systems.* Association for Information Systems.

Rios, R. E., & Riquelme, H. (2010). Brand equity for online companies. *Journal of research in interactive marketing*, 214-240.

Wang, Y., & Herrando, C. (2019). Does Privacy Assurance on Social Commerce Sites Matter to Millennials? *International journal of information management*, 164-177.

Ayaburi, E. W., & Treku, D. N. (2020). Effect of penitence on social media trust and privacy concerns: The case of. *International Journal of Information Management*, 171-181.

Singer, P., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What everyone needs to know.* New York: Oxford University Press.

Ranger, S. (2020, Feb 3). *What is the IoT? Everything you need to know about the Internet of Things right now*. Retrieved from ZDnet: https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/

Ortner, C., Sinner, P., & Jadin, T. (2018). The history of online social media. In I. M. Neels Brugger, *The sage handbook of web history* (pp. 372-384). Sage Publications.

Hootsuite. (2022). *Digital 2022 - Social Media Marketing and Management Dashboard.* Retrieved from Hootsuite: https://www.hootsuite.com/resources/digital-trends

Salvatori, L., & Marcantoni, F. (2015). Social Commerce: A Literature Review. *Science and Information Conference* (pp. 257-262). Core.

Mzekandaba, S. (2021, July 8). *Online shopping boom leads to social commerce*. Retrieved from ITWeb: https://www.itweb.co.za/content/KWEBbvyZA547mRjO

Research and markets. (2022, April). *South Africa Social Commerce Market Intelligence and Future Growth Dynamics Databook*. Retrieved from Research and Markets: https://www.researchandmarkets.com/reports/5578550/south-africa-social-commerce-market-

intelligence?utm_source=CI&utm_medium=PressRelease&utm_code=tz65mw&utm_campaign=1701206+-+South+Africa+Social+Commerce+Market+Intelligence+Report+2022%3a+Market+is+Expe

Lowes, S.-J. (2021). *The Rise of Social Commerce.* Ogilvy.

USAGov. (2022, July 8). *Identity Theft*. Retrieved from USAGov: https://www.usa.gov/identity-theft

Ellipsis. (2021, June 9). *Cybercrimes Act*. Retrieved from Ellipsis: https://www.ellipsis.co.za/cybercrimes-act-19-of-2020/#:~:text=Cybercrimes%20Act%2C%2019%20of%202020,processing%20of%20unlawfully%20intercepted%20data

Sohaib, O. (2021). Social Networking Services and Social Trust in Social Commerce: A PLS-SEM Approach. *Journal of Global Information Management*, 23-44.

Othman, A. K., Hassan, L. F., Hamzah, M. I., Saim, A. R.--.-M., Ramli, M. S., Osman, M. A., & Azhar, M. A. (2019). The Influence of Social Commerce Factors on Customer Intention to Purchase. *Asian Themes in Social Sciences Research*, 1-10.

Anjum, S. &. (2019). The Impact of Social Media Characteristics on E-Commerce Use Behavior Among Youth in Developing Countries. *International Journal of Information Systems and Change Management*. Retrieved from https://www.researchgate.net/publication/336284371_The_Impact_of_Social_Media_Characteristics_on_E-Commerce_Use_Behavior_Among_Youth_in_Developing_Countries

Bölükbaşı, İ. (2021, August 3). *Social Commerce vs. eCommerce: What are the differences?* Retrieved from Threesixtee: https://www.threesixtee.co.uk/social-commerce-vs-ecommerce-what-are-the-differences/

Wang, C. &. (2012). The Evolution of Social Commerce: The People, Business, Technology, and Information Dimensions. . *Communications of the Association for Information Systems. 31.* , 105-127.

Ashoer, M. (2016). The Impact of Perceived Risk on Consumer Purchase Intention in Indonesia; A Social Commerce Study. *Proceeding of the International Conference on Accounting, Management, Economics and Social Sciences (ICAMESS).* Jakarta.

He, W. (2012). A review of social media security risks and mitigation techniques. *Journal of Systems andInformation Technology*, 171-180.

McFarlane, G. (2021, November 4). *How Facebook (Meta), Twitter, Social Media Make Money From You*. Retrieved from Investopedia: https://www.investopedia.com/stock-analysis/032114/how-facebook-twitter-social-media-make-money-you-twtr-lnkd-fb-goog.aspx#:~:text=The%20primary%20way%20social%20media,before%20social%20media%20companies%20existed.

Leetaru, K. (2018, December 15). *What Does It Mean For Social Media Platforms To "Sell" Our Data?* Retrieved from Forbes: https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/?sh=52271fda2d6c

Squires, D. (2016, October 24). *Money and Social Media*. Retrieved from University of Southern California: https://scalar.usc.edu/works/everything-you-always-wanted-to-know-about-social-media-but-were-too-afraid-to-ask/money-and-social-media

Mitrou, L., Kandias, M., Stavrou, V., & Gritzalis, D. (2014). *SOCIAL MEDIA PROFILING: A PANOPTICON OR .* Athens: Athens University of Economics and Business.

Bansal, G., & Chen, L. (2011). If they Trust our E-commerce Site, Will They Trust our Social Commerce Site Too? Differentiating the Trust in E-commerce

and S-commerce: The Moderating Role of Privacy and Security Concerns. *MWAIS Conference Proceedings.* Association for Information Systems.

Hill, M., & Swinhoe, D. (2021, July 16). *The 15 biggest data breaches of the 21st century*. Retrieved from CSO Online: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Government Gazette. (2013). *Protection of Personal Information Act*. Retrieved from South African Government: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

Simpson Attorneys. (2021, August 3). *Does my social need to be POPI compliant?* Retrieved from Mandy Simpson Attorneys: https://www.simpsonattorneys.co.za/does-my-social-media-have-to-be-popia-compliant/

Ross, C., Orr, E. S., Sisic, M., Arseneault, J. M., Simmering, M. G., & Orr, R. R. (2009). Personality and motivations associated with Facebook use. . *Computers in human behavior*, 578-586.

Molinillo, S., Liébana-Cabanillas, F., & Anaya-Sánchez, R. (2018). A Social Commerce Intention Model for Traditional E-Commerce Sites. *Journal of Theoretical and Applied Electronic Commerce Research*, 80-93.

Ayaburi, E. W., & Treku, D. N. (2020). Effect of penitence on social media trust and privacy concerns: The case of Facebook. *International Journal of Information Management*, 171-181.

NIST. (2018, April). *Cybersecurity Framework.* Retrieved from NIST: https://www.nist.gov/cyberframework

Alshibly, H. H. (2015). Customer Perceived Value in Social Commerce: An Exploration of Its Antecedents and Consequences. *Journal of Management Research*, 17-37.

Hair, J. J., Matthews, L., Matthews, R., & Sarstedt, M. (2017). PLS-SEM or CB-SEM: updated guidelines on which method to use. *Int. J. Multivariate Data Analysis*, 107-123.

Hair, J., Hult, G., Ringle, C., & Sarstedt, M. (2022). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM).* Sage Publishing.

Joseph F. Hair Jr., G. T. (2021). *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R A Workbook.* Springer.

Hair, J. F. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM).* Sage Publications.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences.* Lawrence Erlbaum Associates.

Henseler, J. R. (2016). Testing measurement invariance of composites using partial least squares. *International Marketing Review*, 405-431.

Zhou, T., Lu, Y., & Wang, B. (2013). Examining the influences of mobile commerce environment, trust and risk on purchase behavior: Field study in China. *Journal of Electronic Commerce Research*, 180.

Lu, B., Fan, W., & Zhou, M. (2016). Social presence, trust, and social commerce purchase intention: An empirical research. *Computers in Human Behavior*, 225-237.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Gudergan, S. (2017). *Advanced Issues in Partial Least Squares Structural Equation Modeling.* Sage Publications.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). *A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents.* Decision Support Systems.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319-349.

Pavlou, P. A. (2003). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model . *International Journal of Electronic Commerce*, 101-134.

Chen, J., & Dibb, S. (2010). Consumer trust in the online retail context: Exploring the antecedents and consequences. *Psychology and Marketing*.

Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems*, 343-354.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2018). When to use and how to report the results of PLS-SEM. *European Business Review*, 1-24.

Joseph F. Hair Jr., G. T. (2021). *artial Least Squares Structural Equation Modeling (PLS-SEM) Using R: A Workbook.* Springer Cham.

Krasnova, H., Veltri, N. F., & Günther, O. (2017). Privacy calculus on social networking sites: Explorative evidence from Germany and USA. *International Conference on System Sciences*, 1-10.

Martin, K., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 36-58.

Ackerman, M. S., & Donald T. Davis, J. (2003). Privacy and Security Issues in E-Commerce. In D. C. Jones, *New Economy Handbook.* Elsevier, Academic.

Beran, T., & Violato, C. (2010). Structural equation modeling in medical research: a primer. *BMC Res Notes 3*.

Chin, W. W. (1998). Issues and Opinion on Structural Equation Modeling. *MIS Quarterly*, 7-16.

Dinulescu, C. C., Visinescu, L. L., Prybutok, V. R., & Sivitanides, M. (2021). Customer Relationships, Privacy, and Security in Social Commerce. *Journal of Computer Information Systems*, 1-13.

Hajli, M. (2012). Social Commerce Adoption Model. *UK Academy for Information Systems Conference Proceedings.*

Ilmudeen, A. (2019). *Factors Influencing Consumers' Trust on E-commerce Adoption in Sri Lanka.* Jaffna.

Protection of Personal Information Act 4 of 2013. (2022). Retrieved from South African Government: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013popi.pdf

APPENDIX A – Research Instrument

Item	Question	Entry type	Values
1	Age	Number range	1-100, increments of 10
2	Gender	Text	Male/Female/Other
3	On which social media platforms are you active	Checklist	Facebook/Instagram/LinkedIn/Twitter/Other
4	For how long have you been using social media?	Selection	1-3 years, 4-7 years, 8-10 years, more than 10 years
5	Per month, how often do you purchase goods or services using social media?	Number range	1-5 6-10, more than 10
6	How would you rate your general knowledge of social media security and privacy threats?	Selection	Novice, Low, Medium, High, Expert

	Social media attitude (Ross, et al., 2009)	Entry type	Values
7	"Social Media is part of my everyday activity"	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
8	“I am proud to tell people I am on Social Media”	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
9	“I dedicate part of my daily schedule to Social Media”	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree

10	“I feel out of touch when I haven’t logged on to Social Media in a while”	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
11	“I feel I am part of the Social Media community”	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
12	“I would be sad if any of my favourite Social Media shut down”	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree

	Social trust – adapted from (Ayaburi & Treku, 2020)	Entry type	Values
13	I trust my social network's reviews of products available to purchase on social media platforms	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
14	My social network is discerning and well-informed on products and services	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
15	My social network is well informed about security in social media	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
16	My social network is well informed about privacy in social media	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
17	My social network readily shares information about their social commerce experiences	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
18	I value the opinion of my social network's experiences over my own judgement	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
19	I actively seek suggestions from my social network prior to going shopping	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
20	I share my shopping experiences on social media	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree

21	I trust my social network's reviews over those on digital commerce sites, such as Takealot.com and Amazon.com	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
22	I trust SM for providing personalised information	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
23	I always feel confident while interacting in SM communities that I can rely on their responses & feedback	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
24	I feel safe in my postings with SM	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
25	I search information on SM because find it more trustworthy	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
26	I trust information written by others on SM	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree

	Security risk awareness	Entry type	Values
27	I am aware of identity theft as a risk on social media	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
28	I use a strong password to secure my social media accounts	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
29	I use multi-factor authentication to secure my social media accounts	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
30	I only connect to social media using a secure internet connection, e.g., using HTTPS, a virtual private network or equivalent	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
31	I trust social media platforms with my payment information, e.g., credit card information	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree

32	I am aware of online payment scams and fake suppliers on social media	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
33	I take care in validating social media suppliers prior to sharing any sensitive information	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
34	Transacting on social media is higher risk than using other e-commerce sites, e.g. Takealot.com	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
35	I place strong reliance on the community reviews of products and suppliers available to purchase on social media	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
36	I research the social media platform's security policy before deciding if I should purchase	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
37	I have an expectation that the social media platform will remedy fraudulent transactions	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
38	I am selective about which social media platforms I will trust to transact on	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
39	I differentiate between social media platforms based on my level of trust in their online security capability	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
40	I can identify scams designed to steal my social media login credentials	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
41	I validate links in social media posts and emails prior to clicking on them, especially shortened URLs	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
42	I validate browser extensions prior to installation on my device	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree

	Privacy risk awareness	Entry type	Values
43	I am aware of the provisions of the South African Protection of Personal Information Act as it pertains to social media	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
44	I trust suppliers on social media with my personal information	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
45	I research suppliers on social media's privacy policy and notices as part of the purchase process	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
46	Sharing personal information with suppliers on social media is higher risk than with other e-commerce sites, e.g., Takealot.com	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
47	I limit the amount and types of personal information I share on social media	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
48	I limit the sharing of my personal information with the social media platform's partners and affiliates	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
49	I monitor my online accounts for notifications of data breaches that may expose my personal information	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
50	I am aware of the risks imposed by using social login features to access other websites and services	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
51	I am aware of my "right to be forgotten" by social media platforms	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree
52	I research my social network's privacy experiences as part of my purchase process	Likert scale	Strongly disagree, disagree, neutral, agree, strongly agree