AOSIS

Make personal information security great again: A case of users' perspectives on personal identifiable information in South Africa

CrossMark
click for updates

Authors:
Kavish Rajkumar[1]
Kennedy Njenga[1]

Affiliations:
[1]Department of Applied Information Systems, University of Johannesburg, Johannesburg, South Africa

Corresponding author:
Kennedy Njenga,
knjenga@uj.ac.za

Background: There is concern that information technology (IT) users are not taking cognisance of personal information security (PIS), with many keen to disclose personal identifiable information (PII) across connected and integrated IT systems that use the Internet. Compromised PII has led to many users being vulnerable to information security risks emanating from malicious software and hackers.

Objective: This article elicits perspectives from IT users in the metropole area of Johannesburg, South Africa, in an effort to raise awareness of the dangers of oversharing PII across the Internet.

Methods: The study uses a quantitative approach to elicit data on user perspectives. The quantitative data were collected through online surveys distributed amongst IT employees working across various companies in Johannesburg.

Results: The results revealed that of the four constructs drawn from the literature review, namely *training*, *interest*, *awareness* and *action* that possibly predict user predisposition to maintain information security at a personal level, of concern is that only the construct *interest* would not likely predict PIS.

Conclusion: Dangers such as identity theft and phishing attacks are exacerbated by the willingness of users to overshare PII across social networks. A concerted user awareness campaign to promote user PIS needs to be revisited whilst incorporating innovative ways to raise interest amongst users regarding these dangers. South African companies are encouraged to invest resources in bespoke ways to increase user interest, which would be seen as an ideal starting point to making PIS great again.

Keywords: personal identifiable information; personal information security; South Africa; users; IS threats.

Introduction and background

Many large and mid-sized companies in South Africa have automated their operational processes using advanced technologies to make them more competitive. For example, airlines in South Africa have automated the booking process, collecting large amounts of information regarding potential customers. Customers can conveniently make online bookings, with the trade-off being to pass on identifiable information such as names, dates of birth, ages and addresses to access and use these systems. In the South African airline industry and elsewhere, these systems capture what are known as passenger name records (PNRs) (Taplin 2021). The PNR data are mostly captured when users want to transact a business with a company via online or, at times, offline services. The potential for PNRs to be exploited has been a long-established security concern understood by scholars (Argomaniz 2009), and in more recent times, scholars have used PNR as a basis for security governance across transnational borders, using algorithmic regulation (Ulbricht 2018).

In other South African business contexts outside of the airline industry, online tools such as LinkedIn are widespread platforms where much of people's personal information (similar to PNRs) are elicited. The information shared by users can be used to build personal e-profiles that can at times bear full names and addresses, meant to boost online social presence and discoverability (Adriaanse & Rensleigh 2017). The adverse effect of not adequately protecting information was exemplified by Chigada and Madzinga (2021). Van Niekerk (2017) reported that there had been a consistent rise in cyberthreats, mainly threats associated with data breaches and particularly from cybercriminals as reported by Motlhabi et al. (2022). It was also reported that in

South Africa, Life Healthcare, an organisation that holds a tremendous amount of healthcare data (primarily personal health data), was attacked by cybercriminals (Chigada & Madzinga 2021).

Personal identifiable information to personal information security

The PNR data and personal health data can be considered as broadly falling under the category of personal identifiable information (PII), where a user can be identified using a combination of available information and by piecing together data that can distinguish and be traced back to a specific individual (Venkatadri et al. 2018). Many see the sharing of PII data such as PNRs and other personal data on online platforms as posing an information security risk. According to a survey conducted by Grobler, Jansen van Vuuren and Zaaiman (2011), the South African level of personal security awareness of their PII is low, with many sharing PII unknowingly using smartphones (Li & Chen 2010).

Exploiting and commercialising personal identifiable information

Notwithstanding personal security concerns, PII has been of benefit to many companies who have found ways to leverage this for commercial purposes. Studies have shown that PII can be monetised and have commercial value (Da Veiga & Swartz 2016). Companies can use PII for targeted marketing campaigns, improved business intelligence and strategic advantage (Zenda, Vorster & Viega 2020). Personal identifiable information is considered a tradable commodity, and new markets are emerging to trade such valuable information (Spiekermann et al. 2015). In 2018 the European Union launched its General Data Protection Regulation (GDPR), which is now considered to be the world standard for information security and controlling how PII is used or commercialised. The GDPR provides the user with the power to control PII that is collected by organisation (Satariano 2018). In South Africa, there was legislation promulgated on the 19th of November 2013, known as the Protection of Personal Information (POPI) Act, meant to protect individual PII collected, stored and processed by both public and private companies, which took effect in 2021 with the grace period elapsing in 2022 (Taplin 2021). The POPI Act prohibits companies from using PII for direct marketing without consent (Zenda et al. 2020). The POPI Act takes cognisance of personal information such as users' gender, health, race, sex, religion, disability, age and education (Mabeka 2018). The *POPI Act* is regulated through the Information Regulator, a government body that has oversight on the misuse of personal information and will discipline a violation of the Act (Sekgweleo & Mariri 2019).

Need for research in addressing personal information security

Many systems and processes in current use in South Africa have evolved in manner and mode regarding how PII is collected, stored and processed. In the advent of the COVID-19 pandemic, South Africans have witnessed data PII collection initiatives stemming from the pandemic mitigation measures. From swabs taken for COVID-19 testing to vaccines, modern technology has required that PII records be mapped for swabs and PII for each specific person uniquely. Each health record is easily retrievable from a quick response (QR) code that can be carried by the person, either in print form or on an electronic device such as a phone. The QR system has had the advantage of fast readability and great storage, and therefore it is easy for companies to retrieve PII quickly and easily. It is this (albeit controversial) system that has popularised PII for control, such as institutionalised vaccination policies where PII health records can quickly be retrieved.

There have been a lot of changes since Grobler's et al. (2011) study and survey on awareness of personal security of PII data and the impact this has had on both people and companies. This research work, therefore, builds on Grobler et al.'s (2011) work. This research is unique because it introduces the concept of personal information security (PIS) as a mitigating measure for security threats to PII. Personal information security is a construct of security awareness that considers how public and private companies use PII that is deemed very sensitive and must be protected. Sensitive PII can be distinguished from other PII because unauthorised use of sensitive PII can be hazardous and will endanger personal security and property, damage personal reputation or cause mental health issues or embarrassment because of identity theft or blackmail (McCallister 2010).

Research objective

There is a justifiable need to address perspectives regarding PII elicited from South African users, many of whom might be oblivious of the risk of oversharing PII across online platforms. The research objective is to therefore consider how South African users perceive PII and to draw from literature constructs that inform this perception. The constructs drawn from literature can then be tested with results informing policymakers on how to manage PIS better whilst making the often-overlooked personal privacy and security measures great (again) from a user perspective. Following on the research objective, we deconstruct how PII has evolved because of the changes in business operations and argue that it is necessary to determine the current understanding of PIS in light of the dangers articulated when sensitive PII falls into the wrong hands. By addressing user perspectives of PIS within the South African context, we can gain deeper insights into managing PII better and complying better with regulations such as the *POPI Act*.

To meet the stated research objective, we present the research as follows: the introduction has set contexts for the concerns around PII and, importantly, why it is necessary to protect personal information and encourage PIS. A review of literature then follows after the introduction section and points to the ongoing discourse

TABLE 1: Theoretical literature review on personal information security.

Author	Region	Thematic area of study	Theoretical construct
Arthur (2021)	South Africa	Information legislation awareness of undergraduate university students	Awareness
Chigada and Madzinga (2021)	South Africa	Rise in cyberattacks and threats during COVID-19	Action
Grobler et al. (2011)	South Africa	Cyber security awareness in South Africa	Awareness
Nenungwi and Garaba (2022)	South Africa	Knowledge management awareness in provincial government departments	Awareness
Mabeka (2018)	South Africa	E-technology on law of civil procedure	Interest
Motlhabi et al. (2022)	South Africa	Creating context-aware cyberthreat intelligence	Awareness
Phaladi and Ngulube (2022)	South Africa	Need for training and investment in information and knowledge management practices	Training
Staunton and De Stadler (2019)	South Africa	Cyberincidents analysis on protection of information	Interest
Zenda et al. (2020)	South Africa	Need to protect personal information used by marketers	Interest

regarding PII and PIS in the case of South Africa. The methodology section that follows the literature review outlines how we elicited user perspectives surrounding PIS and provides an account of how we developed a theoretical model that is anchored on literature for testing. We present quantitative methods and show how these methods are applied in research. The data analysis section points to how data were collected and analysed to test the model using computerised software, with the implication of results being discussed in the penultimate sections. The conclusion is provided in the last paragraph, followed by an acknowledgement of participants who contributed to this research work.

Literature review

We carried out a theoretical literature review that placed a focus on theoretical constructs examining PIS within the South African context. Whilst there have been previous theoretical literature review studies on information security (Weishäupl, Yasasin & Schryen 2015), none has focused on PIS. Our theoretical literature review is meant to establish the current thematic areas South African scholars have addressed and, importantly, develop new hypotheses in PII and predict its influence on PIS. Our focus was guided by South African scholars and contexts where PII has been addressed such as Phaladi and Ngulube (2022), who espoused information and knowledge protection ideas and insights regarding the security of corporate know-how through the knowledge-based view (KBV) and Chigada and Madzinga's (2021) notable concern on the rise in cyberattacks and threats during the COVID-19 pandemic because of users' inadvertence to information security. Our theoretical literature review was to elicit from studies the constructs that would likely predict PIS as a dependent construct determined through examining users' perspectives. We searched online databases using the search criteria 'information security' and 'South Africa' on freely available databases subscribed to by our host university that included Emerald, IEEE Xplore, Sabinet African Journals, SAGE Journals Online, ScienceDirect, Scopus and SpringerLink. Our search results identified theoretical constructs common in the literature that predict how users deal with PIS: training, interest, awareness and action. We show this in Table 1 and discuss each of these theoretical constructs in detail in the following section.

Training

Widespread cyberattacks use PII in the form of phishing attacks where untrained and unwitting users whose personal data have already been compromised are tricked by a well-orchestrated plan that implores and takes advantage of trust. The key denominator is to persuade the cybervictim to click on a link which, in many circumstances, is the channel through which malicious software (malware) enters the targeted user's computer. Often emails may be perceived as genuine but are not (Gupta, Singhal & Kapoor 2016). Users' PII may be likely compromised when cyberattackers look for information that users are sharing on their online platforms, such as Facebook and LinkedIn. Information elicited from these platforms (such as where they spend time off work or who they socialise with) can be aggregated to build a user profile, which then serves as a basis for a targeted phishing attack because, over time, the cyberattacker has painted a picture of the user. Personal identifiable information can then be used to craft a specific email deliberately designed to manipulate the user and make them think it is genuine Bier and Prior (2014). At times, the use of PII can be adverse when the cyberattack leads to identity theft or social engineering to exploit the user's emotions to gain information (Abawajy 2014). Social engineering often occurs when an attacker manipulates or persuades users by using psychology to give confidential information unintentionally or intentionally (Aldawood & Skinner 2018). Employees are often perceived as weak links in the information security chain and many do not observe PIS at the level expected (Guhr, Lebek & Breitner 2019). The South African National Standard (SANS) has proposed standards that companies can use as guidelines for instituting bespoke information security awareness programs. SANS states that "a very important aspect is lacking, which is the human control of a human firewall" (Murire et al., 2021, p 1). The South African National Standard considers that the smaller the company is, the more likely that it may not institute information security awareness campaigns for its employees. Indeed, smaller companies may most likely have only one employee multitasking in creating controls, who may be constrained to make follow-ups if controls placed are violated. For larger companies, training and awareness have been observed to leverage PIS. It is from this understanding that we propose the following hypothesis.

H1: Training of users will influence personal information security positively.

Interest

The proliferation of social media platforms has created numerous forms of business opportunities from commerce and recruitment to online services such as LinkedIn. According to Da Veiga and Swartz (2016), when a user purchases a product or service, shares information on online services or even enters a competition, their personal information is collected and used by the various companies. Therefore, users have little to no control over their information regarding how it is stored or used. A study by Poushter, Bishop and Chwe (2018) identified that over 50% of adults own a smartphone capable of accessing and transacting on the Internet, with about 43% of adults actively using social media sites. The same study showed that South Africans aged over 18 and under 60 presented the most significant percentage of mobile Internet users.

A study (Arthur 2021) showed that young South Africans concluded that students' knowledge of the acceptance of legislation such as the POPI Act or the regulatory requirements such as the Regulation of Interception of Communication Act (RICA) was not of great importance. Whilst Arthur (2021) reported that 95% of South Africans were RICA registered, many were unaware of RICA requirements. We therefore propose the following hypothesis:

H2: Interest by users will influence personal information security positively.

Awareness

Nenungwi and Garaba (2022) postulate that knowledge management awareness is lacking amongst public sector organisations (PSOs), many of which are 'unable to adapt to the rapidly changing society surrounding them' (p. 1). Despite the apparent benefits of modern and evolving technologies and infrastructure, the potential cybersecurity threats have evolved in tandem, leaving users unaware of these new emergent threats. Users constantly engage with activities online, and with the added pressure of disclosing PII, their vulnerability has increased as they share more information online. Cybercriminals can harvest such information for nefarious reasons. Abawajy (2014) has argued that practices such as excessive sharing of information may compromise even the strongest of the information security initiatives and could be the weak link in the information security chain. Attackers will exploit this weak link to gain access and compromise the internal network. User awareness regarding PII protection has not seemed to progress at the same rate as the evolution and use of technology. Studies on awareness as a construct of behavioural influencers were first highlighted by Rogers (1975), who developed the protection motivation theory (PMT), which predicted peoples' engagement in risk prevention. Building on the

works of Rogers' PMT, Hanus and Wu (2016) studied the impact of user awareness on desktop security awareness using PMT. They found that security awareness significantly affects elements of PMT. From these studies, much emphasis has been placed on designing security awareness programmes that can be designed from PMT. Whilst most studies have considered awareness at the general institutional level, we extend this thinking to users at a personal level and postulate that awareness can be a construct to consider when the focus is given to PIS and propose the following:

H3: Awareness will influence personal information security positively.

Action

Many South African companies are shifting towards adopting cloud computing. One of the reasons given is adopting a new work model, such as working from home, in the advent of the COVID-19 pandemic. Remote working is now popular with many companies. Even though South Africa is steadily easing restrictions, companies have realised that hybrid models that incorporate onsite and work-from-home prove to be popular and cost-efficient. As hybrid models become popular, users find that they store more PII on the cloud to save storage space on their home devices. Although it is often implied that cloud computing has many benefits, some question the total privacy and confidentiality of data that is stored in the cloud. As pointed out, the critical risk is the human actions that lead to the use of cloud computing resources, notably described as the weakest link (Aleem, Wakefield & Button 2013). Human activity has an array of elements, including errors and mistakes made and inadvertent omissions of tasks that ultimately may lead to security risk, not only to the companies but also to employees:

H4: Actions of users will influence personal information security positively.

Theoretical framework

From the given discussions, we have developed a theoretical framework that points to the possible factors that would lead to a better PIS posture. The theoretical framework is shown in Figure 1.

Research design and methodology

To test the theoretical framework depicted in Figure 1, we carried out quantitative research (Goertzen 2017). We outline the quantitative approach as the scientific research advocating for a proper approach to investigating claims. Once appropriate investigations are carried out and claims are supported, practical solutions to social problems can be found. The research made use of a 5-point Likert scale questionnaire that tested the four constructs shown in Figure 1 elicited from the literature review.
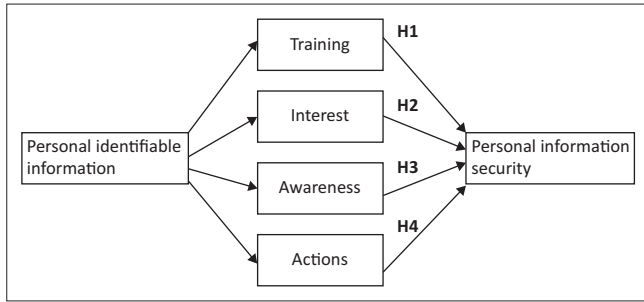
FIGURE 1: Possible factors leading to improved personal information security.

Research approach

The research used a deductive positivist approach to answer the 'what' and 'why' quantifiable types of questions (Hjalmarson & Moskal 2018). The research was also descriptive in the sense that the population and situations were objectively elicited and accurately and systematically tested.

Population sampling

The population sample was centred on employees using IT across the city of Johannesburg, considered the most prominent commercial hub in South Africa, which attracts those working with IT systems. The online survey research method was used, targeting over 100 employees around Johannesburg in two phases. Online surveys were useful because advancements in technology enabled these to be deployed online. The LinkedIn platform focusing on IT professionals was used to solicit responses. The first phase solicited help from 30 participants and the second phase solicited help from 70 participants after a preliminary review of feedback obtained from the first phase. The second phase assured the importance of incorporating experts in possession of specialists' skills and knowledge in IT and information security to provide valuable data (Creswell & Creswell 2017). We computed the sample size using online scientific software developed by Raosoft (2004) that followed the following criteria:

$$x = Z(c/100)2r(100-r) \qquad \text{[Eqn 1]}$$
$$n = N\, x/((N-1)E2 + x) \qquad \text{[Eqn 2]}$$
$$E = Sqrt[(N - n)x/n(N-1)] \qquad \text{[Eqn 3]}$$

Our population size N was used to determine our sample, from a margin of error E. Our estimate of E used a 5% margin of error, and using a fraction of responses (r), we were interested in obtaining Z and critical value for the confidence interval (c) of 95%; thus, we were able to estimate our sample size of 100.

Questionnaire design

As pointed out earlier, our closed-ended questionnaire used a 5-point Likert scale that was distributed online using Google Forms. The questionnaire consisted of the following sections:

1. Biographical questions about the participant.

2. Questions that elicit insights regarding participants' perspectives of personal information security.
3. Questions that test the variables of *training*, *interest*, *awareness* and *actions*.

Section 1 was used primarily to filter out vulnerable participants who, for purposes of meeting and addressing the ethical requirements for the study, needed to be protected. In this regard, only participants meeting the requirements of being more than 18 years of age and those not older than 65 years of age were incorporated in the study. The questions asked were all original and pertained to the four constructs drawn from the literature that helped us formulate these original questions. Whilst Krause (2002) suggested that questions may essentially come from three sources, namely from existing scales, modified scales or from scratch, in our case, our questions were developed from scratch. As our objective was to elicit various user perspectives relating to how they understood PII and the effect this had on PIS, the questions were designed accordingly.

Research procedure and analysis of data

Whilst we acknowledged that there would have been many methods that would have been ideal for collecting data, we restricted ourselves to adopting the above-discussed methods deemed appropriate for a quantitative methodology study. The data obtained were analysed using the Statistical Package for the Social Sciences (SPSS) software tool. The software allowed the data collected from Google Forms to be analysed because it was easy to import it into SPSS without incurring any errors.

Ethical considerations

Ethical clearance was granted by the university where the study was domiciled. A web link was given to study participants for consent to be obtained before commencement. All participants were informed prior to the study that their involvement was voluntary in the cover letter issued to them. No participant was forced to complete the questionnaire. Each participant was also informed that the data collected from the study was to be strictly kept confidential between the researcher and participant.

Data analysis
Online participation and information security awareness

The first section of the questionnaire sought to obtain the participant's demographic profile. The distribution of the gender shows that men comprised 60% of participants, whilst women comprised 36.67% of participants. The participants' age demographics was also considered, and the findings showed that the majority of the participants were aged between 19 and 29 years (53.33%). Those aged between 30 and 39 years comprised 16.67% of participants whilst those aged between 40 and 59 comprised 30% of participants. The study participants

TABLE 2: The questions and averages from participants in the questionnaire.

Question	Discussion	Value (%)	Mean
How often do you share or post information online (WhatsApp status, Instagram, Facebook, other online services, etc.)?	Once every day or more in a week. Of research concern was how much data personal data were being revealed by participants daily regarding PII.	53.0	4.00
Have you ever found a virus or Trojan on your personal computer or other devices?	**Yes:** Participants had an operational knowledge of the risk of a virus or Trojan. Of research concern was the 46% who did not.	56.0	2.07
Do you know how to tell if your computer is hacked or infected?†	**No:** Participants did not know at the current state the level of risk exposure to virus or Trojan infection or whether their systems were compromised. Of research concern was the 46% who did not.	56.0	3.27
Is antivirus currently installed, updated and enabled on your computer or devices?†	**Yes:** Participants had taken security measures to protect their devices. Of research concern was the 10% who did not.	90.0	1.23
Do you know who to contact in case you are hacked or if your computer is infected?†	**Yes:** Participants were aware of the contact person in case of a security breach. Of research concern was the 10% who did not.	50.0	2.87
Can you use your own personal devices, such as your mobile phone, to transfer or share work related information?	**Yes:** This is of research concern because 70% of participants use unprotected personal devices, which are vulnerable and could compromise corporate networks.	70.0	4.13
My friends and family would not send me anything malicious or scams through email or external hard drives.	**True:** Participants held a naïve optimism that their friends and families' systems were not compromised to the level of distributing malicious software. This was of great concern to the research.	86.7	4.47
If you format a hard drive (such as a USB) or erase the files on it, all the information on it is permanently lost.†	**True:** Participants believed that formatting a hard drive completely erases all files stored. This was naïve optimism that is of concern to the research.	83.3	4.33
A hacker would never be interested in me or my devices.	**Neutral:** Participants held the viewpoint they their PII might not be useful, and this was of concern to the research.	30.0	2.77
I do not post anything that will cause me to be a victim of identity theft.	**Neutral:** Participants did not recognise their level of exposure to external threats and the value of their PII. This was of concern to the study.	46.0	2.33
I am interested in increasing my information security knowledge and skills.	**Neutral:** Participants expressed indifference to taking measures for personal information security (PIS), which was of concern to the study.	46.0	2.73
My passwords are strong enough. Nobody can guess them. I am security conscious.	**Agreed:** Participants held a naïve optimism that their passwords were strong. Of concern to the research was the 60% who acknowledged that they passwords they used were not strong.	40.0	3.63

This question was excluded from further analysis as it did not load onto our component model (principal component analysis shown in Table 3).†

TABLE 3: Exploratory factor analysis.

Question	Component				
	1	2	3	4	5
Component matrix†					
Action: Have you ever found a virus or Trojan on your personal computer?	-	-	-	0.557	-
Action: I do not post anything that will cause me to be a victim.	-	-	-	0.570	-
Training: Can you use your own personal devices such as your mobile phone?	-	-	0.715	-	-
Training: How often do you share post information online?	-	-	0.715	-	-
Interest: A hacker would never be interested in me or my devices.	0.784	-	-	-	-
Interest: I am interested in increasing my information security knowledge.	0.640	-	-	-	-
Personal information security: My passwords are strong enough. Nobody can guess them. I am security conscious.	-	0.694	-	-	-
Awareness: My friends and family would not send me anything malicious.	-	-	-	-	0.582
Extraction method: Principal component analysis.					

†, Five components extracted.

were also questioned about their qualifications, and participants holding bachelor's degrees comprised the majority of participants with 43.33% of the sample size. Those with a South African matric qualification comprised 30% of the sample whilst few held a diploma, comprising 26.67% of the sample.

The second part of the questionnaire elicited insights regarding participants' predispositions regarding PIS. The questions ranged from how active they were online to whether they conscientiously shared information that would reveal details about themselves online. Table 2 points to how the participants responded.

Reliability analysis

We carried out an exploratory factor analysis to identify relationships between constructs as suggested by (Fabrigar & Wegener 2011). We present results in Table 3. From the results, we then carried out reliability analysis using Cronbach's alpha to measure the closeness and significance of

relationships the constructs had with each other (Bland & Altman 1997). Generally, acceptable levels of reliability should show Cronbach's alpha values between 0.6 and 0.8 or higher, indicating good levels (Bland & Altman 1997). Values for our constructs' tests fell within this range, suggesting good levels.

Kaiser–Meyer–Olkin test and Bartlett's test of sphericity

The Kaiser–Meyer–Olkin (KMO) carried out on the constructs reflected a significant level of less than 0.05, indicating that the constructs to be tested were useful, and is shown in Table 4.

Questionnaire analysis

We observed that the participants had operational risk awareness regarding posting PII on social platforms, but more worrisome was that these were in the minority. The majority did understand that they needed to take precautionary measures to use social media responsibly, but calls for reliable protection of PII went unheeded. For

TABLE 4: Kaiser–Meyer–Olkin and Bartlett's test.

Kaiser–Meyer–Olkin and Bartlett's test	
Kaiser–Meyer–Olkin measure of sampling adequacy	0.794
Bartlett's test of sphericity	
Approximately chi-square	88.002
df	66.000
Sig.	0.000

df, Degree of freedom; Sig, Significant at the 0.001 level.

TABLE 5: The results of the correlation analysis.

Model	Unstandardised coefficients		Standardised coefficients	t	Sig.
	B	Standard error	Beta		
Coefficients†					
Training	0.399	0.208	0.374	0.337	0.013
Interest	0.089	0.238	0.080	1.214	0.832
Awareness	0.411	0.166	0.364	0.112	0.031
Action	0.476	0.262	0.410	0.115	0.024

Sig, Significant at the 0.001 level.

†, Dependent variable: Personal information security.

instance, 46% of participants said they were interested in information security knowledge and skills, with 86.7% holding a wrong belief that friends and family would not send anything malicious through email or by sharing external hard drives.

Regression analysis

This part of the research examined the proposed model and interpreted regression results carried out using SPSS, a statistical software. Guided by Dhakal (2018), we carried out a multiple linear regression with personal information security as a dependent variable and training, interest, awareness and action as independent variables to infer a causal relationship with these variables. The results are shown in Table 5, and we discuss these in the discussion section that follows.

Figure 2 is a visual representation of the regression analysis.

Discussions

Figure 2 confirms our observation from the cross-tabulation analysis by indicating that participants lacked interest in PIS. Whilst the three other constructs correlate to PIS, it remained of concern that interest does not correlate with PIS. According to Figure 2, training has a positive correlation coefficient, $\rho = 0.374*$ to PIS, demonstrating that when organisations initiate good training campaigns, these can effectively increase PIS awareness and improve PIS. The construct awareness also had a positive correlation coefficient, $\rho = 0.364*$. As mentioned in the previous sections, the lack of interest will hinder employees of an organisation from protecting themselves in the best possible way. Indeed, as pointed out in Figure 2, the correlation coefficient, $\rho = -0.80$ for interest is not significant. Finally, we also observed that correct effort and measures by both the organisation and system users would yield positive results in testing the construct action. Indeed, as Figure 2 points out, actions have a positive correlation coefficient, $\rho = 0.410*$.
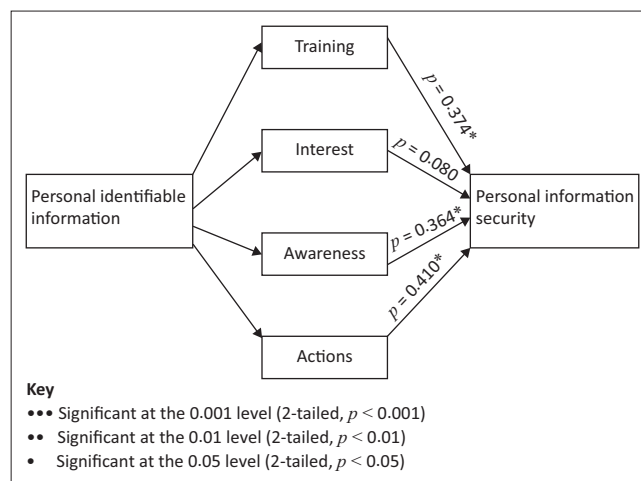
FIGURE 2: Results of analysis.

Based on the data analysis, we can conclude that the study participants' knowledge of PIS is inadequate. More effort is needed to encourage PIS to become a pertinent part of South African organisations' overall information security strategy. We have shown that there is still a long way to go to enable users to be interested in their security of information and avoid oversharing PII data across social platforms by striking a balance between using online tools and protecting PII. We believe this balance can be achieved.

Implications of theory

There have been many studies that guide South African organisations on the best information security management measures to be taken on risk prevention methods. However, few studies have focused on fostering interest amongst users regarding PIS. We bring this important theoretical understanding to the fore whilst adding this to the body of knowledge. By shedding light on the level of interest participants have in PIS, we believe better information security strategies can be designed.

Implications to practice

The model provides guidance to organisations within and outside of South Africa to prioritise the construct of *interest* as the main hindrance to effective information security practices. By understanding interest it is possible to approach information security management differently whilst encouraging users and employees to be co-creators of policies that keep their and their organisations' information secure.

Study limitations and suggestions for future studies

We believe that whilst the study was more quantitative, with the testing of constructs, we believe the limitations of the quantitative approach can be complemented by a study that applies qualitative methods. The qualitative approach can delve deeper and provide deep insights into the reasons why people overshare information on social media platforms and why they are disinterested in PIS.

Conclusion

To conscientise users on the importance of PIS and make this belief great again, it is paramount that organisations foster interest. The study's objective was to show that the oversharing of PII would be detrimental to achieving the desired security of a person's information. We have demonstrated this by carrying out a quantitative study and reporting the results. South Africans could be at risk when they overshare information on online platforms, mainly because new and advanced technologies make it easy for external threats from hackers to compromise on PII. With the growth of social networking platforms and the need for user validation using personal information, the challenge of PIS is exacerbated. We hope this work raises that awareness and offers a way that South African companies can start thinking about increasing interest in information security.

Acknowledgements

References

Adriaanse, L.S., & Rensleigh, C., 2017, 'E-visibility to enhance knowledge sharing', in *Africa Research Group Conference*, Long Beach Golf and Spa, Mauritius, August 29–31, 2017, pp. 1–12. https://doi.org/10.13140/RG.2.2.17191.24489

Abawajy, J., 2014, 'User preference of cyber security awareness delivery methods', *Behaviour & Information Technology* 33(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

Aldawood, H. & Skinner, G., 2018, 'Educating and raising awareness on cyber security social engineering: A literature review', *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering*, December 4–7, IEEE TALE, Wollongong, NSW Australia.

Aleem, A., Wakefield, A. & Button, M., 2013, 'Addressing the weakest link: Implementing converged security', *Security Journal* 26(4), 236–248. https://doi.org/10.1057/sj.2013.14

Argomaniz, J., 2009, 'When the EU is the "Norm-taker": The passenger name records agreement and the EU's internalization of US border security norms', *European Integration* 31(1), 119–136. https://doi.org/10.1080/07036330802503981

Arthur, J., 2021, 'The information legislation (PAIA, POPI, RICA) awareness of undergraduate university students: A longitudinal study', *South African Journal of Information Management* 23(1), a1363. https://doi.org/10.4102/sajim.v23i1.1363

Bier, C. & Prior, J., 2014, 'Detection and labeling of personal identifiable information in e-mails', in N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A.A. El Kalam & T. Sans (eds.), *IFIP International Information Security Conference*, Springer, Berlin, Heidelberg, June, 2014, pp. 351–358. https://doi.org/10.1007/978-3-642-55415-5_29

Bland, J.M. & Altman, D.G., 1997, 'Statistics notes: Cronbach's alpha', *BMJ* 314, 572. https://doi.org/10.1136/bmj.314.7080.572

Chigada, J. & Madzinga, R., 2021, 'Cyberattacks and threats during COVID-19: A systematic literature review', *South African Journal of Information Management* 23(1), a1277. https://doi.org/10.4102/sajim.v23i1.1277

Creswell, J.W. & Creswell, J.D., 2017, *Research design: Qualitative, quantitative, and mixed methods approaches*, Sage Publications, Los Angeles, CA.

Da Veiga, A. & Swartz, P., 2016, 'PoPI Act-opt-in and opt-out compliance from a data value chain perspective: A South African insurance industry experiment', *Proceedings of the 15th International Information Security for South Africa Conference,* IEEE, Johannesburg, South Africa, Aug 17–18, 2016, pp. 9–17.

Dhakal, C., 2018, 'Interpreting the basic outputs (SPSS) of multiple linear regression', *International Journal of Science and Research* 8(6), 1448–1452.

Fabrigar, L.R. & Wegener, D.T., 2011, *Exploratory factor analysis*, Oxford University Press, Oxford, U.K.

Goertzen, M.J., 2017, 'Introduction to quantitative research and data', *Library Technology Reports* 53(4), 12–18.

Grobler, M., Jansen van Vuuren, J. & Zaaiman, J., 2011, 'Evaluating cyber security awareness in South Africa,' *Proceedings of the 10th European Conference on Information Warfare and Security,* The Institute of Cybernetics at the Tallinn University of Technology Tallinn, July 7–8, 2011, Estonia, p. 9.

Guhr, N., Lebek, B. & Breitner, M.H., 2019, 'The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory', *Information Systems Journal* 29(2), 340–362. https://doi.org/10.1111/isj.12202

Gupta, S., Singhal, A. & Kapoor, A., 2016, April, 'A literature survey on social engineering attacks: Phishing attack', in *2016 international conference on computing, communication and automation (ICCCA)*, IEEE Xplore, April 29–30, 2016, Greater Noida, India, pp. 537–540.

Hanus, B. & Wu, Y.A., 2016, 'Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective', *Information Systems Management* 33(1), 2–16. https://doi.org/10.1080/10580530.2015.1117842

Hjalmarson, M.A. & Moskal, B., 2018, 'Quality considerations in education research: Expanding our understanding of quantitative evidence and arguments', *Journal of Engineering Education* 107(2), 179–185. https://doi.org/10.1002/jee.20202

Krause, N., 2002, 'A comprehensive strategy for developing closed-ended survey items for use in studies of older adults', *The Journals of Gerontology: Series B* 57(5), S263–S274. https://doi.org/10.1093/geronb/57.5.S263

Li, N. & Chen, G., 2010, 'Sharing location in online social networks', *IEEE Network* 24(5), 20–25. https://doi.org/10.1109/MNET.2010.5578914

Mabeka, N.Q., 2018, 'The impact of e-technology on law of civil procedure in South Africa', Doctoral dissertation, University of South Africa.

McCallister, E., 2010, *Guide to protecting the confidentiality of personally identifiable information*, vol. 800, no. 122, Diane Publishing, Collingdale, PA.

Motlhabi, M., Pantsi, P., Mangoale, B., Netshiya, R. & Chishiri, S., 2022, 'Context-aware cyber threat intelligence exchange platform', *International Conference on Cyber Warfare and Security* 17(1), 201–210. https://doi.org/10.34190/iccws.17.1.42

Murire, O.T., Flowerday, S., Strydom, K. & Fourie, C.J.S., 2021, 'Narrative review: Social media use by employees and the risk to institutional and personal information security compliance in South Africa', *Journal for Transdisciplinary Research in Southern Africa* 17(1). https://doi.org/10.4102/td.v17i1.909

Nenungwi, F. & Garaba, F., 2022, 'Knowledge management awareness in South African provincial government departments: The case of KwaZulu-Natal Department of Public Works, Pietermaritzburg', *South African Journal of Information Management* 24(1), a1456. https://doi.org/10.4102/sajim.v24i1.1456

Phaladi, M. & Ngulube, P., 2022, 'Mitigating risks of tacit knowledge loss in state-owned enterprises in South Africa through knowledge management practices', *South African Journal of Information Management* 24(1), a1462. https://doi.org/10.4102/sajim.v24i1.1462

Poushter, J., Bishop, C. & Chwe, H., 2018, *Social media use continues to rise in developing countries but plateaus across developed ones*, vol. 22, pp. 2–19, Pew Research Center, Washington, DC, viewed 13 October 2022, https://medienorge.uib.no/files/Eksterne_pub/Pew-Research-Center_Global-Tech-Social-Media-Use_2018.06.19.pdf.

Raosoft, 2004, *Sample size calculator*, Raosoft, Inc. Seattle, WA, viewed 07 June 2002, from http://www.raosoft.com/samplesize.html.

Rogers, R.W., 1975, 'A protection motivation theory of fear appeals and attitude change', *Journal of Phycology* 91(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Satariano, A., 2018, *GDPR, a New Privacy Law, Makes Europe World's Leading Tech Watchdog,* The New York Times, NY.

Sekgweleo, T. & Mariri, M., 2019, 'Critical analysis of PoPI Act within the organisation', *International Journal of Computer Science and Information Security (IJCSIS)* 17(9), 64–69.

Spiekermann, S., Acquisti, A., Böhme, R. & Hui, K.L., 2015, 'The challenges of personal data markets and privacy', *Electronic markets* 25(2), 161–167.

Taplin, K., 2021, 'South Africa's PNR regime: Privacy and data protection', *Computer Law & Security Review* 40, 105524. https://doi.org/10.1016/j.clsr.2020.105524

Ulbricht, L., 2018, 'When big data meet securitization. Algorithmic regulation with passenger name records', *European Journal for Security Research* 3(2), 139–161. https://doi.org/10.1007/s41125-018-0030-3

Van Niekerk, B., 2017, 'An analysis of cyber-incidents in South Africa', *The African Journal of Information and Communication* 20, 113–132. https://doi.org/10.23962/10539/23573

Venkatadri, G., Andreou, A., Liu, Y., Mislove, A., Gummadi, K.P., Loiseau, P. et al., 2018, 'Privacy risks with Facebook's PII-based targeting: Auditing a data broker's advertising interface,' in *2018 IEEE Symposium on Security and Privacy (SP)*, IEEE, San Francisco, CA, 21–23 May, 2018, pp. 89–107.

Weishäupl, E., Yasasin, E. & Schryen, G., 2015, 'A multi-theoretical literature review on information security investments using the resource-based view and the organizational learning theory', *Proceedings of the International Conference on Information Systems - Exploring the Information Frontier*, ICIS 2015, Fort Worth, Texas, USA, 13–16 December, 2015.

Zenda, B., Vorster, R. & Viega, A.D., 2020, 'Protection of personal information: An experiment involving data value chains and the use of personal information for marketing purposes in South Africa', *South African Computer Journal* 32(1), 113–132. https://doi.org/10.18489/sacj.v32i1.712