South African Journal of Information Management
ISSN: (Online) 1560-683X, (Print) 2078-1865

A model on workarounds and information security integrity

Authors:
Kennedy Njenga[1]
Ntsakisi F. Nyamandi[1]
Mmatshuene A. Segooa[2]

Affiliations:
[1]Department of Applied Information Systems, College of Business and Economics, University of Johannesburg, Johannesburg, South Africa

[2]Department of Informatics, Faculty of Information & Communication Technology, Tshwane University of Technology, Tshwane, South Africa

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

Dates:
Received: 18 Mar. 2024
Accepted: 09 July 2024
Published: 30 Aug. 2024

How to cite this article:
Njenga, K., Nyamandi, N.F. & Segooa, M.A., 2024, 'A model on workarounds and information security integrity', *South African Journal of Information Management* 26(1), a1853. https://doi.org/10.4102/sajim.v26i1.1853

Background: Workarounds are creative human actions that bypass a known problem in a system or a policy. Workarounds serve as temporary 'fixes' when effective but will often compromise the integrity of information systems in the long term, mainly when they are ineffective.

Objectives: Forming part of behavioural studies in information systems security, the study aimed to investigate how workarounds influence the integrity of information security systems across businesses.

Method: A quantitative approach that followed the positivism paradigm was employed. A survey strategy was used, and data were collected using closed-ended questionnaires targeting employees working in the Gauteng province of South Africa. The survey elicited responses from 207 professional participants. Analysis was done using Statistical Package for Social Sciences (SPSS) v29 software.

Results: The study suggests that *Individuality* and *Job characteristics* are crucial predictors of workarounds, with the most notable findings pointing to a significant positive association between *Workaround* and *Information security integrity.* Crucially, highly individualistic employees are more likely to initiate workarounds, and in turn, this influences information security integrity.

Conclusion: The work shows that employees with highly individualistic personalities are more likely to initiate workarounds and should be trained and supervised to mitigate this attribute, as this might be detrimental to information security integrity.

Contribution: The study contributes theoretically by showing how workaround activities influence information security integrity. This study will assist enterprises in fortifying their information security measures.

Keywords: workarounds; information security; integrity; behaviour; non-compliance.

Introduction

The importance of information security in the context of human behaviour in modern organisations cannot be understated and remains crucial (Aksoy 2024). Understanding the socio-technical aspects of information security in organisations is necessary because human behaviour poses a high risk to the integrity of information security. Humans are often perceived as the weakest link in the information security chain (Daudi 2023), and targeted remedial measures are necessary to raise users' awareness of this.

Human behaviour may introduce inherent information security risk particularly when such behaviour is exemplified in workarounds. Workarounds are creative human actions that bypass a known problem in a system or a policy. An employee may engage in workarounds to overcome any emergent challenge or limitation exposed by a system or process, and these workarounds will at times have a significant impact on the *integrity*, *confidentiality* and *availability* of protected data.

Study context

In early 2010, in a study by Kyobe (2010), the authors raised concerns about compliance with information security policies across universities in South Africa. Twenty years later, Murire et al. (2020) cited a lack of awareness as a major contributor to non-compliance across South African businesses. As recently as this year, Mugwagwa Bhero and Chibaya (2024) pointed out that some of the strategies that should be implemented to curb cybersecurity threats include a 'focus on compliance'. The Gauteng province hosts two large cities which include, Johannesburg, the largest city and Pretoria, the capital city. Gauteng attracts multinational and national financial institutions and businesses that are targets of serious cybercrimes, with employees playing a big part in contributing to cybersecurity risks. Employee behaviour across these institutions was raised as a concern. Workaround behaviour across businesses in Gauteng, South Africa, that are seen as contributing to non-compliance with information security policies and, therefore, contributing to risk is explained in the next section.

Workarounds and compliance

Workarounds refer to employees' ability to seek solutions to problems through bypassing policies when these policies are not perceived to be working. In efforts to circumvent an established information security protocol or procedure and initiate a workaround, an employee may introduce a system weakness known as a vulnerability that can be, at a later stage, exploited by an attacker with nefarious intentions. It is, therefore, necessary to understand what individual, cultural or institutional factors motivate employees to carry out workarounds. This research endears to the following problem:

Problem statement

Adhering to information security policies is central to good information security practices (Siponen 2006). Unfortunately, workarounds seen as a form of non-complaint information security behaviour are becoming common because of perceived benefits (Azad & King 2008). Little is known regarding why this is so. This research explores the reasons behind this trend, with a focus on how workarounds threaten the integrity of information systems.

Research objectives

Considering the concern scholars raise regarding the non-compliance behaviour that characterises workarounds, this research undertook to examine the following:

1. Carry out a literature review to gain an understanding of what are the factors that drive workarounds in workplaces.
2. Develop a model that explains these factors, propose and test hypotheses derived from this model.
3. Derive insights from the testing of this model that can add value and contribute to the body of knowledge on how organisations can manage workarounds and strengthen compliance of policies.

This research is therefore structured as follows: Section one has outlined the context of research and articulated the research problem and research objectives. Section two that follows examines the literature regarding workarounds, and the impact this behaviour has on the integrity of information. Section three explains the research methodology used in this study, and the penultimate sections discusses how data were analysed and the results that followed. The conclusion follows thereafter presenting the research work's contribution and way forward.

Literature review

This section provides a literature review of Information Security Integrity. A systematic literature review identified factors drawn from behavioural sciences that specifically focus on workaround behaviour. Based on these factors, six hypotheses were formulated and proposed. These factors were identified using a non-biased and scientific approach. The university under which this study was domiciled has subscribed to the following databases that assisted the researchers in identifying the relevant literature: *ACM Digital Library*, *ProQuest*, *Emerald Management*, *IEE Explore*, *Scopus* and *ScienceDirect*.

The search works included 'information integrity', 'factors influencing integrity,' 'information security behaviour', 'information security workarounds' and 'risk-in-workarounds'. Various literature that presented factors that influence workarounds and how workarounds pose a security risk to information security integrity were included in this study. Table 1 summarises the outcome of this systematic literature review process.

Table 1 offers a comprehensive summary of pertinent literature that provides insights regarding the factors that are most likely to influence workarounds. These factors are discussed in depth in the subsequent sections.

Information security integrity

Confidentiality, integrity and availability (CIA) triad forms the fundamental basis for information security that stresses information protection against unauthorised access, alteration or destruction (Liu et al. 2020). Part of maintaining information integrity requires that measures to protect information by reducing breaches through continuous monitoring, secure authentication practices and training to raise user awareness (Da Veiga & Martins 2015). Studies point to the advancing of understanding regarding information integrity and the

TABLE 1: Information security integrity factors (researcher).

Constructs	Authors
Information security integrity	Liu, Wang and Liang (2020), Harley and Cooper (2021), Harley and Cooper (2021), Colwill (2009), Wong et al. (2019).
Workarounds	Alter (2014), Woltjer (2017), Rooney et al. (2021), Slabbert, Thomson and Futcher (2021), Van Offenbeek et al. (2024)
Self-efficacy	Hameed and Arachchilage (2021), Rhee, Kim and Ryu (2009), Tamjidyamcholo et al. (2013).
Individuality	Twenge and Campbell (2018), Locke and Latham (2002), Kshetri (2017), Chua, Awaworyi Churchill and Koestner (2020), Huuskonen and Vakkari (2013).
Information processing capability	Wei, Chen and Rice (2023), Beerepoot et al. (2019a), Alshammari (2023), Beerepoot, Van de Weerd and Reijers (2019b).
Collegiality	Freedman (2012), Sharpe, Lounsbery and Templin (1997), Bissett and Saunders (2015).
Job characteristics	D'Arcy, Hovav and Galletta (2009), Alter (2014), Huang et al. (2016).

Note: Please see full reference list of the article for more information.

protection of data, but a crucial concern has been the organisations lack a way of standardising this understanding. Many scholars talk of information integrity (Harley & Cooper 2021) or of data integrity (Duggineni 2023), which mostly considers similar aspects. It is, therefore, crucial that the integrity of information be better understood. Studies point out that human factors such as behaviour may compromise the integrity of information, particularly those employees working in the organisations (Wong et al. 2019). The next section details some of these human factors specifically focusing on workaround behaviour.

Workarounds

Though mentioned in management, organisational and technology literature, workarounds are under theorised in information security literature. The theory of workarounds postulated by Alter (2014) explains workarounds in organisational settings, pointing to how these occur and, importantly, assists management efforts in policy compliance (or non-compliance). Woltjer (2017) has pointed out that workarounds-as-improvisation correlated with information systems expertise, and although those skilled individuals intended to achieve work quality and integrity, the unintended consequence was non-compliance as the trade-off. Indeed, scholars have raised the concern that the trade-offs in workarounds, bypassing established policies and procedures, may constitute an information security risk (Slabbert et al. 2021). Workarounds overwhelm information security practitioners in organisations because they may not know which policies have been violated and how they have been violated when workarounds are initiated. When employees are under pressure because of time or lack of resources and initiate workarounds, this is often detrimental to information security integrity (Van Offenbeek et al. 2024). Workarounds primarily stem from personality traits such as self-efficacy or organisational traits such as culture and collegiality (Rooney et al. 2021), propagating shortcuts to tasks. To this end, the following hypothesis is proposed:

H1: Workarounds will predict information security integrity.

Self-efficacy

Self-efficacy theory places a great emphasis on the importance of how individuals perceive their own abilities. In information systems research, studies show that employees with stronger 'self-confidence for tackling IS security threats are more likely to adopt [information system] IS security innovation' (Hameed & Arachchilage 2021). While in some parts, this innovation may be of important to the organisation, most times it is not, because the workaround was performed outside of policy and regulation. Self-efficacy most often influences intention and may result in abuse of computer systems tasks (Rhee et al. 2009). Self-efficacy may benefit organisations when employees are confident in themselves to initiate practical remedies against attempted information security breaches, finding solutions but staying within the limits of policy guidelines. According to Tamjidyamcholo et al. (2013), self-efficacy positively impacts the ability to identify and successfully respond to security threats and compliance. At times, the individual may lack self-regulating mechanisms that override these policies. This is where self-efficacy becomes detrimental. To this end, the following hypothesis is proposed:

H2: Self-efficacy will predict workaround behaviour.

Individuality

Individuality places greater emphasis on the independence and rights of individuals than collective entities. The idea of individuality fosters personal freedom and the pursuit of personal goals with minimal intrusion from external forces (Twenge & Campbell 2018). Locke and Latham (2002) state that individual attitudes advance effective goal-setting processes, which enhance employee motivation and job satisfaction by emphasising individual accomplishments rather than group outcomes in performance appraisals. Kshetri (2017) has studied information security integrity in healthcare and observed that integrity might be hindered by individuality because employees might prioritise self-interests over organisational security protocols in their efforts to work around challenges. According to Chua et al. (2020), independence and personal well-being can be promoted through individual cultures but also hinder industry-wide information-sharing initiatives while encouraging competition, leading to a decline in overall safety postures. Another problem is that information system sectors are faced with competition based on culture, which makes it difficult for them to share knowledge about cyber-attacks (Chua et al. 2020). In their study, Huuskonen and Vakkari (2013) examined social workers who undertook workarounds and exhibited individualism by employing small-scale tricks within their Information Technology (IT) department to maintain a continuum of positive trajectory for their clients. Though this saved time, the social workers either ignored policies entirely or merged information, a clear policy violation. To this end, the following hypothesis is proposed:

H3: Individuality will predict workaround behaviour.

Information processing capability

An organisation's ability to gather, interpret, transform and disseminate information is referred to as organisational information processing capabilities (IPC) (Chen & Nath 2018). Employees may sometimes assume that the current systems or procedures do not fit or accommodate their needs, and they often resort to workarounds to 'fix' these processes. The problem is that organisations usually spot abnormalities or patterns that point to potential security breaches if they have the necessary processing power, but this 'fixing' may affect IPC (Wei et al. 2023).

Information processing capability and information security can be affected by issues like increasing data volume and complexity, information system vulnerabilities, poor infrastructure, human error and data protection law compliance (Beerepoot et al. 2019a). As workarounds may cause breaches of business standards that can give rise to unauthorised entry or loss of data because of system restrictions or inefficiencies, among others, they establish extra risks to information security (Alshammari 2023).

Organisations usually confront difficulties in processing information where processes have been 'worked around', and this affects the integrity of information security, as proposed by Beerepoot et al. (2019b). Investing in cutting-edge IT infrastructure and personnel training is necessary to manage the workarounds and foster proper data handling using best practices. Organisations should emphasise compliance with data protection regulations to reduce the risks associated with compromised information integrity. To this end, the following hypothesis is proposed:

H4: Information processing capability will predict workaround behaviour.

Collegiality

Freedman (2012) reviewed the boundaries of collegiality by examining what collegiality means in the context of organisational settings and considered the contradictory and opposing sides of collegiality. Collegial decision-making has been important because of the joint decisions that are to be made regarding resource allocation and support from senior executives or supervisors towards ensuring that organisational goals are met. Supportive leadership and cooperative decision-making are the main drives of collegiality in organisations (Sharpe et al. 1997). Bissett and Saunders (2015) argue that collegiality results from managers and supervisors taking an active role at work and being dedicated to creating a friendly environment that promotes growth, productivity and employee development. To this end, the following hypothesis is proposed:

H5: Collegiality will predict workaround behaviour.

Job characteristics

It is important to understand how job characteristics might influence employee behaviour and workarounds, partly because employees are now faced with an ever-growing reliance on technology and the always-changing information security threat landscape. Task relevance and skill variety, because of the changing technology requirements for tasks, are important job characteristics that have been observed to affect motivation to carry out workarounds (D'Arcy et al. 2009).

Employees may turn to solutions outside of their area of expertise when they feel underutilised or lack a variety of skills (Alter 2014), which could lead to unintentional information security vulnerabilities (Woltjer 2017). As proposed by Huang et al. (2016), organisations should concentrate on neutralising and resolving fundamental job characteristics concerns that would likely lead to workarounds to lessen the negative impact on information security integrity. To this end, the following hypothesis is proposed:

H6: Job Characteristics will predict workaround behaviour.

Research methodology

As a critical component of the research process, the research methodology not only addresses methodically the research issues on hand (Bryman 2016) but also has to be appropriately selected to explain those issues (Galliers & Land 1987). The research methodology entails collecting empirical data using methods such as surveys, interviews and observations (Asenahabi 2019). An important research methodology component is the research ontology and epistemology. Research ontology deals with the nature of reality, while research epistemology directs data gathering and analysis and deals with how knowledge is gathered (Creswell 2014; Hirschheim 1985). Both research ontology and research epistemology are key aspects of well-designed research as these will influence the philosophy, approach, strategy and methods of data collection and analysis. This research takes the positivist approach that recognises research consisting of only data that can scientifically be verified and capable of mathematical-quantitative proof (Goertzen 2017; Hjalmarson & Moskal 2018). The validity and reliability of data are objectively derived from facts, placing a strong emphasis on empirical observation and measurement (Bryman & Bell 2015).

Approach

The rationale for selecting a positivist and objective approach was for the researchers to be able to determine the causal relationship between constructs derived from the literature review: *information security integrity* as the dependent variable with *workaround*. The causal relationship between the independent variables, *self-efficacy*, *individuality*, *collegiality*, *information processing capability* and *job characteristics* with *workaround* was also considered. This called for drawing inferences of these relationships using the deductive approach, beginning with hypotheses development and leading towards the testing of these hypotheses. To this end, an online web-based survey was administered to 207 participants, using online platforms such as LinkedIn and Facebook, targeting participants aged between 18 years and 65 years who resided in Gauteng, South Africa. A purposeful, non-probability sampling strategy was used, with the size determined using Equation 1 provided by Raosoft (2004) as follows:

$$x = Z(c/100)2r(100–r)$$

$$n = N\, x/((N–1)\ E2 + x)$$

$$E = \text{Sqrt}\ [(N - n)\ x/n(N–1)] \qquad \text{[Eqn 1]}$$

Raosoft (2004) designed a web-based, scientific sample size calculator that embeds the above formula, which the researchers applied to determine the optimal sample of 212. The researchers used this recommendation in conjunction with defining the possible number of potential Information Technology professionals in the Gauteng province who met the criteria of the research as 1500 (*N*). Dada et al. (2022) estimated that at least 3355 Information Technology jobs were published by LinkedIn, suggesting that 46.7% (or 1543.4) of these were domiciled in Gauteng. We, therefore, used *N* as 1500 active LinkedIn and Facebook (assuming the same participants used both platforms) IT professionals to be targeted. We applied a 5% margin of error, with a 95% confidence level, and a low response distribution of 20%, resulting in a recommended size of 212. The researchers managed to get 207 participants who completed the web-based survey.

Web-based survey instrument

A study's most important component is gathering data, and there are several ways to do it based on the resources available, the financial implications and the time the researcher must complete (Kothari 2004). With Internet usage proliferating in Gauteng, it would be possible to target these groups of IT professionals using web-based surveys, saving on time and costs and, importantly, uploading data into software for analysis. Web-based surveys have their own benefits, like low costs, quick data gathering and design flexibility (Lawrence Neuman 2014). A Likert scale of five points was used to structure the closed-ended questions on the web-based survey, which was then separated into each of the three sections:

1. Research Background and Participant Consent.
2. Section A, Participant demographics.
3. Section B, Information on users' security behaviour.

Participants who required ethical protection were filtered out using the first two screening questions. A pilot study was carried out using preliminary data from 20 participants to assess the validity of the research instrument and guarantee that bias or impact is minimised.

Data analysis

The collected data were analysed using SPSS (Statistical Package of Social Sciences, version 24). A total number of 207 participant data points was analysed after missing and filtered out data. Participants who did not reply were removed from the study. The initial round of online inquiries aimed to gather demographic information about the participants.

Ethical considerations

Research ethics was a key consideration while developing the data collection instrument, deciding on the approach to use in the research process and, importantly, analysing data. The ethical principles guided the participants' rights in providing data and how data were to be used once collected. The research was granted ethical clearance by the University of Johannesburg and issued with the reference number 2023AIS012.

All participants were required to give their informed consent to participate; the consent included the following:

- Participants would be required to agree to participate in the survey.
- Participants were free to stop participating in the survey at any time.
- Participants were assured of anonymity.

Results

The descriptive statistics of the study participants are presented, depicting the participant's duration of service and the role the participants play in the various industries across Gauteng, South Africa.

Profile of participants: Duration of service

Most of the participants in the sample had over 30 years of IT experience in various IT roles. The distribution of the duration of service suggests that there is a significant presence of experienced IT participants, which suggests a mature workforce. This distribution is as follows: those working for less than 10 years were 20.8%, those working for more than 10 years to 20 years were 15.5%, those working for more than 20 years to 30 years were 28.5%, while those working for more than 30 years were 33.3%. The results are provided in Table 2.

Profile of participants: Role and industry

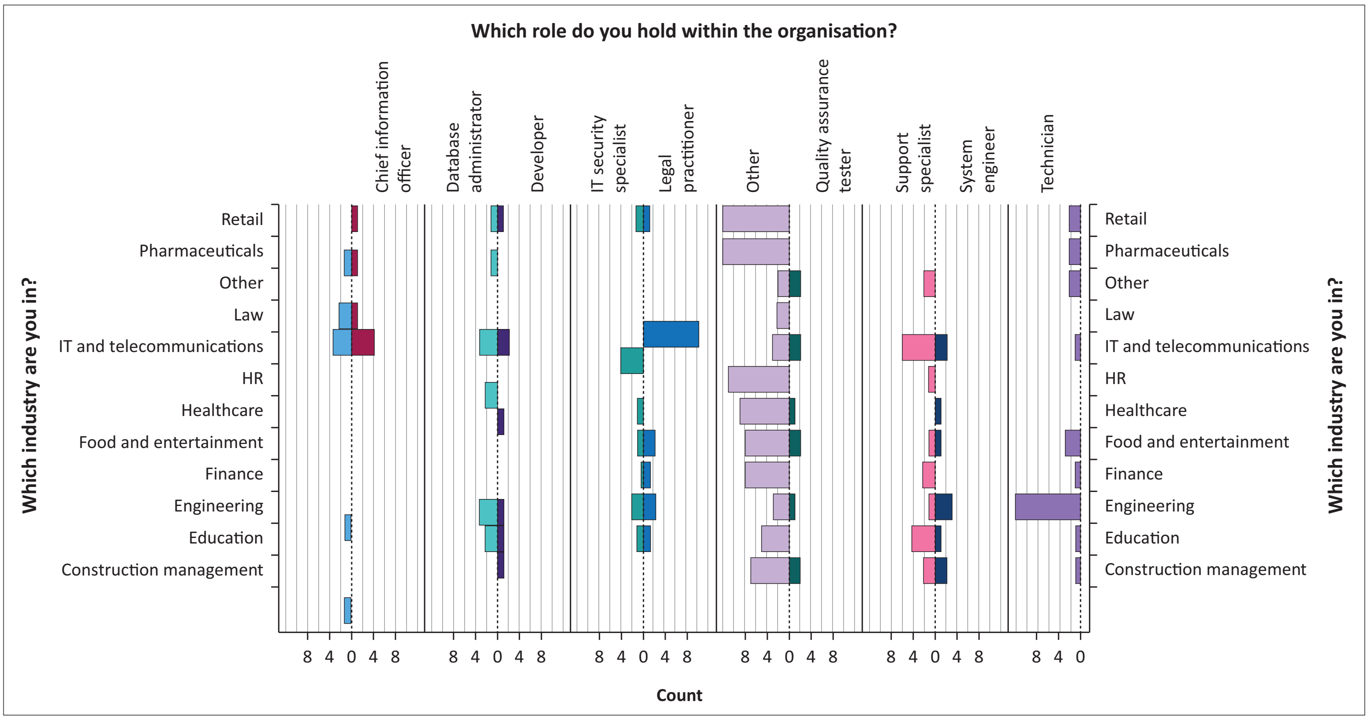
Statistical Package of Social Sciences derived a graphical representation of the role the IT participants played in various industries across Gauteng, South Africa. The shape and size of the various data points for the role in the industry suggest that many of the participants worked in positions that were not generally defined. This is because of the nature of the technological advancements in the field pointing to emerging new roles, particularly in the fields of retail, pharmaceuticals, healthcare and human resources. Most participants with clearly defined roles were technicians who worked in the engineering sector. There were legal practitioners who played a role both in IT and in the legal profession (e.g., forensic experts, eDiscovery specialists, cybersecurity experts and legal IT support) who also participated in the research. These professionals also constituted an averagely higher sample size. The study also sampled a few IT and telecommunication industry chief information officers. The results are provided in Figure 1.

Measurement testing: Common method variance test

Research results may at times be skewed, and this may lead to interpretation errors. One way of addressing this concern

TABLE 2: Duration of service (researcher).

How many years have you been in the industry?				
Valid years	**Frequency**	**%**	**Valid %**	**Cumulative %**
Other-undefined	4	1.9	1.9	1.9
11–20	32	15.5	15.5	17.4
21–30	59	28.5	28.5	45.9
Less than 10	43	20.8	20.8	66.7
More than 30	69	33.3	33.3	100.0
Total	**207**	**100.0**	**100.0**	-



IT, Information Technology; HR, Human Resources.

FIGURE 1: Population pyramid on industry and role (researcher).

is to carry out a common method variance (CMV) test as suggested by Craighead et al. (2011). To see whether CMV was going to be a concern before further analysis was to be carried out. An exploratory factor analysis (EFA) was carried out to see whether there would be any single factor that would account for a substantial portion (more than 50%) of the total variance. Using SPSS EFA generated the total variance explained table shown by Table 3.

Statistical Package of Social Sciences results of the EFA using principal component analysis (PCA) reveal that the first component explained 24.109% of the total variance, followed by the second component explaining 17.476% resulting in a cumulative 41.586% across two components. This falls short of the rule-of-thumb threshold of 50% for one component, and that common method bias would not be a concern for this study. The extraction of the 23 other factors indicates that the variance is distributed across multiple factors, suggesting that further data analysis was possible.

Validity, reliable and factor loading

The degree to which a quantitative analysis test accurately measures a concept is known as validity, while reliability considers the consistency of any conclusions made by the researcher (Street & Ward 2012). The test of sampling adequacy performed by SPSS using Kaiser–Mayer–Olkin's (KMO) measure showed that the KMO was 0.828, with the degree of freedom being 253, significant at < 0.001, confirming that factor analysis would be a good method to reduce underlying variables in the model. Table 4 provides KMO results.

TABLE 3: Total variance (researcher).

Total variance explained

Component	Initial eigenvalues			Extraction sums of squared loadings		
	Total	% of variance	Cumulative %	Total	% of variance	Cumulative %
1	5.54	24.11	24.11	5.54	24.10	24.11
2	4.02	17.48	41.59	4.02	17.48	41.59
3	1.49	6.48	48.06	1.49	6.48	48.06
4	1.37	5.95	54.01	1.37	5.95	54.01
5	1.20	5.24	59.24	1.20	5.24	59.25
6	1.13	4.92	64.16	1.13	4.92	64.16
7	1.03	4.50	68.66	1.03	4.50	68.66
8	0.74	3.23	71.90	-	-	-
9	0.69	2.99	74.89	-	-	-
10	0.63	2.76	77.65	-	-	-
11	0.61	2.64	80.29	-	-	-
12	0.58	2.52	82.81	-	-	-
13	0.53	2.29	85.11	-	-	-
14	0.50	2.17	87.27	-	-	-
15	0.47	2.05	89.33	-	-	-
16	0.45	1.98	91.31	-	-	-
17	0.40	1.73	93.03	-	-	-
18	0.38	1.64	94.67	-	-	-
19	0.34	1.50	96.17	-	-	-
20	0.31	1.35	97.52	-	-	-
21	0.23	0.99	98.51	-	-	-
22	0.21	0.92	99.43	-	-	-
23	0.13	0.57	100.00	-	-	-

Note: Extraction method: Principal component analysis.

To determine how well the factor items (10 questionnaire items) were related to each other and to assess the consistency of the responses to these questions, a reliability analysis that applied Cronbach alpha was matched to the 10 related items.

This Table 5 shows that items that did not load into their components were removed and not included for further analysis. The Cronbach's alpha values were greater than 0.5 are deemed appropriate in information systems research (Street & Ward 2012).

A correlation test was carried out to determine whether there was any association between variables. This was a quick check to see whether further analysis in regression was worthwhile. The results are shown in Table 6.

Table 6 shows association, suggesting a further need to conduct a regression to present, examine and explain the model. The results show that the correlations were not high (close to 1 or –1), suggesting that multicollinearity would not be a major concern.

Examination of the model

The hypotheses to be included in the model were tested using multiple linear regression analysis. This was done to test and determine whether there was an existing relationship between independent variables and the dependent variable, information security integrity (as well as workaround behaviour). Table 7 displays the regression analysis's findings.

The results liner regression results for H1 indicated that the model significantly predicted the variable *Information Security Integrity*, (p < 0.001). It was observed that the predictor variable *Workaround* had a significant positive effect on Information Security integrity (β = 0.340, t = 5.165, p < 0.001). A multiple liner regression was done to test whether the other variables would predict workaround. The results are presented by Table 8.

The results of the multiple liner regression analysis also show that the model significantly predicted *Workaround.* Several predictors contribute to this, specifically *Job Characteristics* (β = 0.315, t = 4.464, p < 0.001) and *Individuality* (β = 0.208, t = 2.867, p = 0.005), which show a positive relationship with Workaround. However, it was observed that *Self-efficacy* (β = –0.150, t = –1.845, p = 0.067), *Information Processing Capability* (β = –0.114, t = –1.473, p = 0.142) and *Collegiality* (β = –0.078, t = –1.091, p = 0.276) did not significantly predict workaround.

Summary of hypothesis testing findings

Findings of the six hypotheses that were tested suggest that *self-efficacy*, *collegiality* and information processing capability are not crucial predictors to workarounds. This can be explained as follows: In the first instance, many organisations are observed to have started training their employees on information security risks that their employees expose their organisations when the employees bypass policies as temporary 'fixes', but in doing so compromise the integrity of information systems. However, because of the individual characteristics of skilled employees, as well as the nature and characteristics of the work they do, chances of experiencing workarounds from those employees remains high. The testing summary results are illustrated in Table 9.

Discussion

Considering that when employees engage in workarounds and bypass policies, the management may be left unaware of what the employees did. These workarounds may lead to new information security vulnerabilities, and management may not be certain how these vulnerabilities arose. This is especially true for employees who exhibit high individualism and the characteristics of their work. The findings that workaround impacts information security integrity are in agreement with Woltjer (2017), who established that workarounds are improvisational acts that are frequently seen in organisations and are seen as non-compliance behaviour. This study, however, did not delve into pointing out how this non-compliance may influence information security integrity. This study adds to these insights. Indeed, as suggested by many information systems studies (Bulgurcu, Cavusoglu & Benbasat 2010; Cheng et al. 2013), policy compliance is a necessary part of information systems governance that monitors procedures to be followed.

TABLE 4: Validity, Kaiser–Mayer–Olkin's and Bartlett's test (researcher).

KMO and Bartlett's test		
Kaiser-Meyer-Olkin measure of sampling adequacy		0.830
Bartlett's test of sphericity	Approx. Chi-square	1819.530
	df	253.000
	Sig.	< 0.001

Approx, approximately; *df*, degrees of freedom; Sig., significance.

TABLE 5: Reliability and factor loading (researcher).

Factor item	10 items (questions) - Factor loading	Loading†	Cronbach's alpha values
Self-efficacy	1	0.67	0.79
	2	0.71	
	3	0.65	
	4	0.57	
	5	0.84	
Individuality	1	0.58	0.78
	2	0.75	
	3	0.78	
	4	0.69	
	5	0.69	
Information processing capability‡	1	0.64	0.83
	2	0.79	
	3	0.87	
	4	0.77	
Job characteristics§	1	0.74	0.51
	2	0.58	
Collegiality¶	1	0.53	0.58
	2	0.51	
	3	0.90	
Workaround behaviour††	1	0.85	0.86
	2	0.88	
Information security integrity‡‡	1	0.89	0.69
	1	0.78	

Note: Extraction method: Principal component analysis. Rotation method: Varimax with kaiser normalisation.

†, Rotation converged in 8 iterations.

‡, 1 item did not load to this component.

§, 3 items did not load to this component.

¶, 2 items did not load to this component

††, 3 items did not load to this component.

‡‡, 3 items did not load to this component.

TABLE 6: Test of correlation (researcher).

Job characteristics	Self-efficacy	Individuality	Information processing capability	Job characteristics	Collegiality	Information security integrity	Workaround
Self-efficacy							
Pearson Correlation	1.000	-	-	-	-	-	-
Sig. (2-tailed)	-	-	-	-	-	-	-
N	206.000	-	-	-	-	-	-
Individuality							
Pearson Correlation	0.221**	1.000	-	-	-	-	-
Sig. (2-tailed)	0.001	-	-	-	-	-	-
N	206.000	206.000	-	-	-	-	-
Information processing capability							
Pearson Correlation	0.596**	0.069	1.000	-	-	-	-
Sig. (2-tailed)	< 0.001	0.324	-	-	-	-	-
N	206.000	206.000	206.000	-	-	-	-
Job characteristics							
Pearson Correlation	-0.057	0.447**	-0.124	1.000	-	-	-
Sig. (2-tailed)	0.412	< 0.001	0.075	-	-	-	-
N	206.000	206.000	206.000	206.000	-	-	-
Collegiality							
Pearson Correlation	0.413**	0.346**	0.314**	0.213**	1.000	-	-
Sig. (2-tailed)	< 0.001	< 0.001	< 0.001	0.002	-	-	-
N	206.000	206.000	206.000	206.000	206.000	-	-
Information security integrity							
Pearson Correlation	-0.227**	0.185**	-0.277**	0.184**	-0.080	1.000	-
Sig. (2-tailed)	0.001	0.008	< 0.001	0.008	0.254	-	-
N	206.000	206.000	206.000	206.000	206.000	206.000	-
Workaround							
Pearson Correlation	-0.222	0.281**	0.253	0.414**	-0.036	0.340**	1.000
Sig. (2-tailed)	0.061	< 0.001	0.020	< 0.001	0.603	< 0.001	-
N	206.000	206.000	206.000	206.000	206.000	206.000	206.000

Sig, significance.

**, Correlation is significant at the 0.01 level (2-tailed).

TABLE 7: Liner regression weights: Hypothesis 1 (H1) (researcher).

Coefficients†					
Model	Unstandardised coefficients		Standardised coefficients	*t*	Sig.
	B	SE	Beta		
(Constant)	3.22	0.33	-	9.87	< 0.001
Workaround	0.34	0.06	0.34	5.16	< 0.001

SE, Standard error; Sig, significance.

†, Dependent variable: Information security integrity.

TABLE 8: Multiple regression weights: Hypothesis 2-6 (H2-6) (researcher).

Coefficients†					
Model	Unstandardised coefficients		Standardised coefficients	*t*	Sig.
	B	SE	Beta		
(Constant)	2.26	0.64	-	3.53	< 0.001
Self-efficacy	-0.16	0.09	-0.15	-1.84	0.067
Individuality	0.32	0.11	0.21	2.87	0.005
Information processing capability	-0.10	0.07	-0.11	-1.47	0.142
Job characteristics	0.46	0.10	0.31	4.46	< 0.001
Collegiality	-0.09	0.09	-0.08	-1.09	0.276

SE, Standard error; Sig, significance.

†, Dependent variable: Workaround.

TABLE 9: Multiple liner regression weights (researcher).

Hypotheses	Factors	*p*	Action
HI	Information security integrity ← Workaround	< 0.001	Accepted
H2	Workaround ← Self-efficacy	0.067	Rejected
H3	Workaround ← Individuality	0.005	Accepted
H4	Workaround ← Information processing capability	0.142	Rejected
H5	Workaround ← Collegiality	0.276	Rejected
H6	Workaround ← Job characteristics	< 0.001	Accepted

Pointing out that individuality may influence workarounds, it follows that highly individualistic personality types are more inclined to bypass formal policies if they think that by doing so, they may likely achieve desired outcomes, following their own methods independent of the organisation. The study findings point to this and show how this can challenge information security integrity. To effectively manage these individuals, organisations should provide the necessary training while advocating cultural changes targeted mostly at highly individualistic employees. Organisations can create policies and procedures that clarify proper conduct regarding policy compliance, perhaps pointing to the information security dangers of workarounds.

Contribution to practice

Workarounds behaviour significantly affects information security integrity, and it remains crucial for management to be aware that this happens. Practitioners can handle information integrity risks necessitated by workarounds through effectively learning, improving user experience and developing a security-conscious culture. This research has brought this understanding to the fore, pointing out that workarounds create vulnerabilities that are potential entry points for those with nefarious intent to exploit. In practice, the existence of the policies is not enough to deter employees' intent on workarounds; however, cultural change and raising awareness would be important starting points. Management may suggest that employees engage in transparency and truthfulness and uphold proper work ethics as they carry out their duties, lessening the need for workarounds.

Contribution to knowledge

While the goal of any research is to address a research issue or problem, this research study points to a crucial concern regarding how workarounds affect information security integrity. Although there is a dearth of work that points to workarounds being a concern, this research adds to the body of knowledge already available in the field of information security but addresses integrity concerns, particularly in the context of the Gauteng province, South Africa. Although the study was carried out in the Gauteng province, which can be a limitation regarding generalisability, the study is grounded in a strong theoretical framework that is applicable across broader contexts. By examining workarounds under this context, the study may assist those interested in the field in understanding how information security vulnerabilities occur. Organisations can, therefore, take the necessary steps, equipped with these insights, to establish training programs.

Limitations and future research

This research study lays a groundwork for future research and decision-making with insights into the dynamic around workarounds. In our study, we found that 'collegiality' did not significantly predict workaround behaviour. This may require further exploration as to why this is so for future research. The research findings provide a standard by which monitoring workaround behaviour can be established. While the work took a quantitative and objective approach, it fell short of new discoveries by asking participants to discuss their lived experiences. Qualitative research would, therefore, provide richer aspects of these lived experiences. Future research should employ qualitative techniques to elicit these insights.

Conclusion

To conclude, this research work underscores an often-overlooked cultural dimension to information security integrity, namely the presence of workarounds in organisational settings. The study has shown, through surveying IT practitioners working and residing in the Gauteng province of South Africa, that workarounds are often present in situations where employees are collegial and tend to have high self-efficacy. This study aligns well with the literature that indicates that workarounds are prevalent and often indicate non-compliance to policies. Overall, the work points to a better understanding of the underlying socio-contextual and cultural underpinnings surrounding individuals who bypass policies to overcome intended goals. This work has provided a good foundation for future studies touching on information security and the constant battle to ensure its integrity.

Acknowledgements

Competing interests

The authors declare that they have no financial or personal relationships that may have inappropriately influenced them in writing this article.

Authors' contributions

K.N. was the main supervisor for the project and conceptualised the work and curated the data. N.F.N. drafted the initial investigation, write-up and reviewed the work. K.N. sent the work to a third reviewed literature. N.F.N. was involved in the conceptualisation, methodology, investigation and writing the original draft. M.A.S. was involved in the methodology and validation of the study.

Funding information

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Data availability

The data that support the findings of this study are available on request from the corresponding author, K.N.

Disclaimer

The views and opinions expressed in this article are those of the authors and are the product of professional research. It does not necessarily reflect the official policy or position of any affiliated institution, funder, agency or that of the publisher. The authors are responsible for this article's results, findings and content.

References

Aksoy, C., 2024, Building a cyber security culture for resilient organizations against cyber attacks. *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi* 7(1), 96–110. https://doi.org/10.33416/baybem.1374001

Alshammari, A., 2023, 'A novel security framework to mitigate and avoid unexpected security threats in Saudi Arabia', *Engineering, Technology & Applied Science Research* 13(4), 11445–11450. https://doi.org/10.48084/etasr.6091

Alter, S., 2014, 'Theory of workarounds', *Communications of the Association for Information Systems* 34, a55.

Asenahabi, B.M., 2019, 'Basics of research design: A guide to selecting appropriate research design', *International Journal of Contemporary Applied Researches* 6(5), 76–89.

Azad, B. & King, N., 2008, 'Enacting computer workaround practices within a medication dispensing system', *European Journal of Information Systems* 17(3), 264–278. https://doi.org/10.1057/ejis.2008.14

Beerepoot, I., Ouali, A., Van de Weerd, I. & Reijers, H.A., 2019a, 'Working around health information systems: To accept or not to accept?', *Twenty-Seventh European Conference on Information Systems (ECIS2019)*, Stockholm-Uppsala, Sweden, June 08, 2014.

Beerepoot, I., Van de Weerd, I. & Reijers, H.A., 2019b, 'The potential of workarounds for improving processes', *Paper presented at the Business Process Management Workshops: BPM 2019 International Workshops*, Vienna, Austria, September 1–6, 2019, Revised Selected Papers 17.

Bissett, N. & Saunders, S., 2015, 'Criticality and collegiality: A method for humanizing everyday practice?', *Journal of Management Education* 39(5), 597–625. https://doi.org/10.1177/1052562914557281

Bryman, A., 2016, *Social research methods*, Oxford University Press, Oxford.

Bryman, A. & Bell, E., 2015, *Business research methods*, Oxford University Press, Oxford.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I., 2010, 'Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness', *MIS Quarterly* 34(3), 523–548. https://doi.org/10.2307/25750690

Chen, L. & Nath, R., 2018, 'Business analytics maturity of firms: An examination of the relationships between managerial perception of IT, business analytics maturity and success', *Information Systems Management* 35(1), 62–77. https://doi.org/10.1080/10580530.2017.1416948

Cheng, L., Li, Y., Li, W., Holm, E. & Zhai, Q., 2013, 'Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory', *Computers & Security* 39(Part B), 447–459. https://doi.org/10.1016/j.cose.2013.09.009

Chua, S.N., Awaworyi Churchill, S. & Koestner, R., 2020, 'Life, liberty and the pursuit of happiness: Examining the role of personal and country-level freedom in well-being', in S. Awaworyi Churchill, L. Farrell, S. Appau (eds.), *Measuring, understanding and improving wellbeing among older people*, pp. 237–263, Palgrave Macmillan, Singapore. https://doi.org/10.1007/978-981-15-2353-3_11

Colwill, C., 2009, 'Human factors in information security: The insider threat–Who can you trust these days?', *Information Security Technical Report* 14(4), 186–196. https://doi.org/10.1016/j.istr.2010.04.004

Craighead, C.W., Ketchen, D.J., Dunn, K.S. & Hult, G.T.M., 2011, 'Addressing common method variance: Guidelines for survey research on information technology, operations, and supply chain management', *IEEE Transactions on Engineering Management* 58(3), 578–588. https://doi.org/10.1109/TEM.2011.2136437

Creswell, J.W., 2014, *Research design qualitative quantitative and mixed methods approaches*, Sage, Los Angeles, CA.

D'Arcy, J., Hovav, A. & Galletta, D., 2009, 'User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach', *Information Systems Research* 20(1), 79–98. https://doi.org/10.1287/isre.1070.0160

Dada, O.A., Obaido, G., Mienye, I.D. & Aruleba, K., 2022, 'The Leading Locations of Information Technology (IT) Jobs in South Africa', *In International Conference on Sustainability in Software Engineering & Business Information Management*, pp. 63–74, Springer International Publishing, Cham.

Daudi, M., 2023, 'Trust framework on exploitation of humans as the weakest link in cybersecurity', *Applied Cybersecurity & Internet Governance* 2(1), 1–26. https://doi.org/10.60097/ACIG/162867

Da Veiga, A. & Martins, N., 2015, 'Improving the information security culture through monitoring and implementation actions illustrated through a case study', *Computers & Security* 49, 162–176. https://doi.org/10.1016/j.cose.2014.12.006

Duggineni, S., 2023, 'Impact of controls on data integrity and information systems', *Science and Technology* 13(2), 29–35.

Freedman, S., 2012, 'Collegiality matters: How do we work with others?', *Journal of Academic Librarianship* 38(2) 108–114.

Galliers, R.D. & Land, F.F., 1987, 'Choosing appropriate information systems research methodologies', *Communications of the ACM* 30(11), 901–902. https://doi.org/10.1145/32206.315753

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

Hameed, M.A. & Arachchilage, N.A.G., 2021, 'The role of self-efficacy on the adoption of information systems security innovations: A meta-analysis assessment', *Personal and Ubiquitous Computing* 25(5), 911–925. https://doi.org/10.1007/s00779-021-01560-1

Harley, K. & Cooper, R., 2021, 'Information integrity: Are we there yet?', *ACM Computing Surveys (CSUR)* 54(2), 1–35. https://doi.org/10.1145/3436817

Hirschheim, R., 1985, 'Information systems epistemology: An historical perspective', *Research Methods in Information Systems* 9, 13–35.

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

Huang, Z., DAngelo, M., Miyani, D. & Lie, D., 2016, 'Talos: Neutralizing vulnerabilities with security workarounds for rapid response', *Paper presented at the 2016 IEEE Symposium on Security and Privacy (SP)*.

Huang, Z., DAngelo, M., Miyani, D. & Lie, D., 2016, 'May. Talos: Neutralizing vulnerabilities with security workarounds for rapid response', in M. Locasto (ed.), *2016 IEEE Symposium on Security and Privacy (SP)*, pp. 618–635, IEEE, San Jose, CA

Huuskonen, S. & Vakkari, P., 2013, '"I did it my way": Social workers as secondary designers of a client information system', *Information Processing & Management* 49(1), 380–391. https://doi.org/10.1016/j.ipm.2012.05.003

Kothari, C.R., 2004, *Research methodology: Methods and techniques*, 2nd edn., New Age International Publishers, New Delhi.

Kshetri, N., 2017, 'Blockchain's roles in strengthening cybersecurity and protecting privacy', *Telecommunications Policy* 41(10), 1027–1038. https://doi.org/10.1016/j.telpol.2017.09.003

Kyobe, M., 2010, 'Towards a framework to guide compliance with IS security policies and regulations in a university', in H.S. Venter, M. Coetzee & M. Loock (eds.), *2010 Information security for South Africa*, pp. 1–6, IEEE, Sandton, Johannesburg.

Lawrence Neuman, W., 2014, *Social research methods: Qualitative and quantitative approaches*, Pearson, Essex.

Mugwagwa, A., Bhero, E. & Chibaya, C., 2024, 'Cybersecurity strategy: Future proof cybersecurity for small to medium enterprises in South Africa', *International Journal of Research in Business and Social Science* 13(4), 15–24. https://doi.org/10.20525/ijrbs.v13i4.3308

Liu, C., Wang, N. & Liang, H., 2020, 'Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment', *International Journal of Information Management* 54, 102152. https://doi.org/10.1016/j.ijinfomgt.2020.102152

Locke, E.A. & Latham, G.P., 2002, 'Building a practically useful theory of goal setting and task motivation: A 35-year odyssey', *American Psychologist* 57(9), 705. https://doi.org/10.1037/0003-066X.57.9.705

Murire, O.T., Flowerday, S., Strydom, K. & Fourie, C.J., 2020, 'Narrative review: Social media use by employees and the risk to institutional and personal information security compliance in South Africa', *TD: The Journal for Transdisciplinary Research in Southern Africa* 17(1), 1–10. https://doi.org/10.4102/td.v17i1.909

Raosoft, 2004, *Raosoft sample size calculator*, viewed 04 July 2024, from http://www.raosoft.com/samplesize.html.

Rhee, H.-S., Kim, C. & Ryu, Y.U., 2009, 'Self-efficacy in information security: Its influence on end users' information security practice behavior', *Computers & Security* 28(8), 816–826. https://doi.org/10.1016/j.cose.2009.05.008

Rooney, M.J., Levy, Y., Li, W. & Kumar, A., 2021, 'Towards assessing password workarounds and perceived risk to data breaches for organizational cybersecurity risk management taxonomy', *Proceedings on Cybersecurity Education, Research and Practice 30th October 2021*, Kennesaw State University, Kennesaw, GA.

Sharpe, T., Lounsbery, M. & Templin, T., 1997, 'Cooperation, collegiality, and collaboration: Reinforcing the scholar-practitioner model', *Quest* 49(2), 214–228. https://doi.org/10.1080/00336297.1997.10484236

Siponen, M., 2006, 'Six design theories for IS security policies and guidelines', *Journal of the Association for Information systems* 7(1), 19. https://doi.org/10.17705/1jais.00095

Slabbert, E., Thomson, K.-L. & Futcher, L., 2021, 'Towards a risk assessment matrix for information security workarounds', in *International Symposium on Human Aspects of Information Security and Assurance*, pp. 164–178, Springer International Publishing, Cham.

Street, C.T. & Ward, K.W., 2012, 'Improving validity and reliability in longitudinal case study timelines', *European Journal of Information Systems* 21(2), 160–175. https://doi.org/10.1057/ejis.2011.53

Tamjidyamcholo, A., Baba, M.S.B., Tamjid, H. & Gholipour, R., 2013, Information security–Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language', *Computers & Education* 68, 223–232. https://doi.org/10.1016/j.compedu.2013.05.010

Twenge, J.M. & Campbell, W.K., 2018, 'Cultural individualism is linked to later onset of adult-role responsibilities across time and regions', *Journal of Cross-Cultural Psychology* 49(4), 673–682. https://doi.org/10.1177/0022022118764838

Van Offenbeek, M.A., Vos, J.F., Van den Hooff, B. & Boonstra, A., 2024, 'When workarounds aggravate misfits in the use of electronic health record systems', *Information Systems Journal* 34(2), 293–326. https://doi.org/10.1111/isj.12478

Wei, S., Chen, X. & Rice, R.E., 2023, 'We can work it out: A multilevel examination of relationships among group and individual technology workarounds, and performance', *Journal of Operations Management* 69(6), 1008–1038. https://doi.org/10.1002/joom.1267

Woltjer, R., 2017, 'Workarounds and trade-offs in information security–An exploratory study', *Information & Computer Security* 25(4), 402–420. https://doi.org/10.1108/ICS-02-2016-0017

Wong, W.P., Tan, H.C., Tan, K.H. & Tseng, M.-L., 2019, 'Human factors in information leakage: Mitigation strategies for information sharing integrity', *Industrial Management & Data Systems* 119(6), 1242–1267. https://doi.org/10.1108/IMDS-12-2018-0546