



Predicting communication constructs towards determining information security policies compliance

**Authors:**

Tsholofelo Rantao¹ 
Kennedy Njenga¹ 

Affiliations:

¹Department of Applied Information Systems, College of Business and Economics, University of Johannesburg, Johannesburg, South Africa

Corresponding author:

Kennedy Njenga,
knjenga@uj.ac.za

Dates:

Received: 26 Feb. 2020
Accepted: 16 July 2020
Published: 12 Oct. 2020

How to cite this article:

Rantao, T. & Njenga, K., 2020, 'Predicting communication constructs towards determining information security policies compliance', *South African Journal of Information Management* 22(1), a1211. <https://doi.org/10.4102/sajim.v22i1.1211>

Copyright:

© 2020. The Authors.
Licensee: AOSIS. This work is licensed under the Creative Commons Attribution License.

Background: Ineffective communication using inappropriate channels and poor listening skills have resulted in poor compliance with information security (InfoSec) policies. Lack of compliance with InfoSec policies minimises employee proficiency whilst also exposing organisations to business risk.

Objectives: This research addresses management's concern regarding why employees do not comply with InfoSec policies and proposes that how policies are communicated is integral to compliance and that effective communication can serve to ameliorate compliance.

Method: The research adopts communication theories from knowledge management, psychology and information systems to draw on important constructs which are then tested in order to identify those that can strongly predict InfoSec policy compliance. The research was quantitative and used a survey to elicit responses from a sample of 100 employees selected from 6 organisations.

Results: Our findings suggest that of the 10 communication constructs used in the miscellany of perception and determinism (MPD) framework, half of these (five) constructs strongly predicated compliance, namely *reasons for communication, media appropriateness, non-conflicting interpretations, feedback immediacy* and *personal focus*. The rest of the constructs were weak predictors or could not predict compliance.

Conclusion: The research advances InfoSec literature by adapting the MPD model as integral to the development, communication and importantly, compliance with InfoSec policies. The MPD model is pertinent as it aggregates theories of communication from a number of academic disciplines and underpinnings not considered before, thereby improving our understanding on how we communicate InfoSec policies for better compliance.

Keywords: information security; policies; compliance; perception theories; determinism theories.

Introduction

Information security (InfoSec) policy formulation and compliance lies at the heart of addressing how personally identifiable information (PII) is treated by organisations (Siponen, Mahmood & Pahnla 2009). Personally identifiable information is any online information relating to identifying a person. However, it is a cause of concern that users of technology are increasingly revealing personal information in an attempt to enhance and ascertain their online presence using tools such as *LinkedIn™* to create e-profiles for discoverability (Adriaanse & Rensleigh 2017a). On 25 May 2018, an important zeitgeist arose that dictated new ways that organisations should adopt to treat personal information (Tikkinen-Piri, Rohunen & Markkula 2018). From this period onwards, the handling and protection of personal information became a concern for the executive board of companies through enactment of privacy laws that protect personal information, specifically the General Data Protection Regulation (GDPR) (Tikkinen-Piri et al. 2018). This prerogative has been daunting considering that advanced knowledge-sharing technologies have resulted to user's e-visibility embodied by online presence on the World Wide Web, making discoverability via e-profiles relatively easy (Adriaanse & Rensleigh 2017b).

It is the relative ease by which PII may be obtained online that compliance with privacy laws has been henceforth considered important in order to protect personal information of the users. Not complying with InfoSec policies can now constitute a business risk (Kandeh, Botha & Botha 2018). *Facebook™* was unfortunately showcased as the first casualty under this requirement for

Read online:

Scan this QR code with your smart phone or mobile device to read online.

non-compliance with GDPR. Lawmakers were angry because *Facebook*TM was reportedly involved in a breach that affected over 87 million individuals worldwide (Isaak & Hanna 2018). *Facebook*TM had failed to justify why their application improperly shared users' personal data with the political consultancy firm *Cambridge Analytica*TM (Isaak & Hanna 2018). Of concern was that *Cambridge Analytica*TM had gained access to *Facebook*TM users' personal data for nefarious reasons such as data harvesting (Sanders & Patterson 2019). In order not to fall victim of GDPR guidelines, organisations have embarked on measures to address business risk by instituting InfoSec policies that prescribe the best way to handle personal data. In South Africa, where this study is domiciled, the right to privacy is granted by the constitution and common law (Borena, Belanger & Dedefa 2015). Common law considers privacy harm carried out to an individual's personhood as wrong. However, the 'personhood' in this definition is highly influenced by the Ubuntu philosophy where not only can a person determine his or her personhood, but so can others (Borena et al. 2015).

InfoSec policies are meant to protect an individual's privacy but studies show that these requirements are overlooked (Poulet 2006). Importantly, the compliance to InfoSec policies has been complicated by the introduction of many mobile devices that users now bring to organisations (Musarurwa & Flowerday 2018). What is troubling as well is that many users neither seem to adhere to, nor follow InfoSec policies regardless of their understanding of the need to do so (Puhakainen & Siponen 2010). Employees at times ignore policies (Vance & Siponen 2012) or even worse, violate policies deliberately (Lowry & Moody 2015). Part of the reason for non-compliance of policies is that there is a disconnect between how policies are communicated, interpreted and implemented (Odine 2015). The direct causes of ineffective communication include poor conceptualisation of policies, using inappropriate platforms to present these policies and poor listening skills (Odine 2015). Communication failure is a major concern that is responsible in-part for non-compliance (Kirlappos, Parkin & Sasse 2014) and less attention has been given in research to the diverse communication approaches that are present.

Need for research in communicating InfoSec policies

This research therefore addresses management's concern for low employee compliance to InfoSec policies using a miscellany of theories that address communication drawn from various disciplines such as knowledge management, psychology and information systems to explain how appropriate communication may ameliorate compliance. As employees are considered the weakest link to the implementation and protection of information across organisations, (Aurigemma 2013) much attention needs to be placed on how InfoSec policies are communicated to this group (Susmilch 2019). By addressing communication, researchers may have a better understanding of why important InfoSec policies are not followed.

Understanding communication in depth would be achieved by identifying theories and developing a framework that addresses the efficacy of the communication process regarding InfoSec policies to users. In this regard, we present a compelling opportunity to model a quantitative framework anchored on selected communication theories and testing this framework. In doing so, firstly, we cautiously consider various communication theories present by reviewing literature and by identifying the main theories that would address our objective. This is done in the following section of this work. Following this, we then formulate the miscellany of perception and determinism (MPD) framework that aggregates discourse regarding communication in such a way as to develop and test hypothesis. We finally outline how MPD can be applied in an organisational setting to encourage proper communication of policies and thus encourage compliance.

Literature review

Information security protects an organisation's information assets from unauthorised access and threats to decrease the level of risk directly connected with those assets (Williams 2001). Infosec cannot be fully effective with only the implementation of technical tools and interventions and requires people to be part of the process (Herath & Rao 2009). For InfoSec to be holistic, it must therefore integrate technology, people as well as processes through a robust InfoSec architecture (Eloff & Eloff 2005), with information and the flexible architecture being regarded as a core capability of the organisation for it to remain competitive (Niemand & Mearns 2020).

Research has drawn a link between corporate InfoSec and compliance leading to competitive intelligence (Fitzpatrick & Burke 2003) with studies proposing that considerable value should be placed on competitive intelligence regarding how this construct can contribute to strategy development, decision-making and enhancing the organisational performance (Du Plessis & Gulwa 2016). What is disconcerting is that, employees undermine organisational performance by not complying with organisational policies (Whitman 2003). Compliance regarding any policy ensures that business processes set out by management are performed as expected (Cannon & Byers 2006). A growing number of organisations are concerned about abiding by statutory provisions in order to avoid fines for non-compliance. Avoiding fines is not the only consideration and proactive organisations aim at continuous improvements of their procedures. Indeed continuous improvement is an issue that many organisations sometimes avoid as it identifies areas lacking business excellence (Mthembu & Du Plessis 2018).

According to Cannon and Byers (2006) addressing compliance as business process is often challenging. Siponen, Mahmood and Pahlila, (2009) hold this view as well and suggest that compliance can be improved if the desired practices and normative expectations are visible to all. As suggested, compliance can be attributed to social pressure and visibility.

Studies show that the visibility of InfoSec policies influences adherence. In particular, social norms significantly shape compliance when InfoSec policies become part of employees' conversations (Siponen et al. 2009). Understanding why employees do not comply with InfoSec policies may be challenging as employees work under different organisational contexts, under different management practices, different laws, regulations and guidelines and at times using different technology. The following section elaborates on literature around compliance with InfoSec policies.

Compliance with InfoSec policies

Attempting to understand compliance has been a subject of research for many years (Vance & Siponen 2012). The majority of the published research has focused on the reasons why users do not comply with InfoSec policies (Posey, Roberts & Lowry 2015). Most of these studies with the exception of a few, do not address the importance of the communication process, as a way to predict compliance. The following InfoSec studies present reasons for not complying (in order of most recent study) as shown in Table 1.

As shown in Table 1, few studies explicitly address the communication process that predict compliance. Most studies address other important considerations. Sharma and Warkentin (2018) as an example, postulated that not complying with InfoSec policies is partly driven by employment status and differentiates between temporary workers and permanent workers, with the former less likely to comply with InfoSec policies because of the level of investment in the organisation. It has also been argued that when InfoSec policies are seen as restrictive, users will tend not to comply in order to re-establish a sense of control that is seemingly lost (Lowry & Moody 2015). Interestingly, past behaviour and the tendency to be conditioned by that behaviour can influence compliance as shown by Lowry and Moody (2015). Work overload and stress has also been a factor that influences compliance as it encourages employees to be morally disengaged with policies (D'Arcy, Herath & Shoss 2014). Personal gain has equally been suggested as a reason for lack of compliance (Hu et al. 2011) and the nature of penalties and sanctions to be meted out (D'Arcy et al. 2009). This latter study partly addresses communication, with the main focus being on how sanctions

and penalties are to be communicated when users violate policies.

Having this in mind, the importance of communication as a predictor of compliance is to be understood in order to minimise any risk business organisations may face for non-compliance. The study therefore endeavours to examine communication more deeply by drawing on useful constructs from theories that can be tested. The following section addresses a miscellany of theories that consider communication in depth, namely media synchronicity theory (MST), communication theory and media richness theory. These three theories present different lenses on the communication process.

Media synchronicity theory

Media synchronicity theory drawn from the discipline of knowledge management and information system advocates for a shared understanding of what is being communicated and requires convergence and conveyance (Dennis, Fuller & Valacich 2008). Understanding convergence and conveyance has been shown to increase communication performance. On the one hand, conveyance is based on the transmission of large amounts of raw information and retrospective analysis. This means that individuals do not have to transmit and process the information at the same time (information processing time). On the other hand, convergence is based on the transmission of higher-level abstraction of information, which requires less deliberation. This means that for individuals with shared mental models, the encoding and decoding of new messages is faster (Dennis et al. 2008). Burke and his colleagues stated that synchronous communication is a significant factor affecting interpersonal communication and teamwork. Various types of media may be used synchronously meaning communication takes place at the same time (Dennis et al. 2008). According to MST, the familiarity of individuals with the duties or activities they are supposed to be performing will affect the relative amounts of convergence and conveyance. Frasier et al. (2019) showed that familiarity and communication will influence each other. We therefore propose the following:

H1: Familiarity of InfoSec policies will predict compliance with InfoSec policies.

TABLE 1: Reasons for lack of compliance with InfoSec policies.

Reason for non-compliance	Explanation	Example in InfoSec Literature	Communication addressed in study
Employment status	Users (temporary workers) considering themselves less invested in the organisation are more inclined not to comply as opposed to permanent workers.	Sharma and Warkentin (2018)	-
Individual reasoning	Users consider InfoSec policies restrictive and reason that non-compliance may help them re-establish control.	Lowry and Moody (2015)	-
Past experiences	Users who are driven by past behavior and are prone to non-compliance will tend to do so.	Lowry and Moody (2015)	-
Moral disengagement	Users who are stressed because of work overload will tend to be morally disengaged leading to non-compliance.	D'Arcy et al. (2014)	-
Benefit	Users who feel that they may gain from non-compliance will do so. The benefits would include thrill and/or happiness.	Hu et al. (2011)	-
Sanctions	Users who consider sanctions for non-compliance as less severe or less certain D'Arcy, Hovav and Galetta (2009) to occur are bound not to comply.		✓

Note: Please see the full reference list of the article, Rantao, T. & Njenga, K., 2020, 'Predicting communication constructs towards determining information security policies compliance', *South African Journal of Information Management* 22(1), a1211. <https://doi.org/10.4102/sajim.v22i1.1211>, for more information.

Research work by Chen, Srinivasan and Mahmassani (1999) showed that information quality and quantity are strong predictors of compliance behavior. Chen and Chang (2018) addressed information quality and contend that quality is an important precursor to understanding value. We use the construct *quality* applied in media synchronicity and propose the following:

H2: Information quality will predict compliance with InfoSec policies.

Early work at the University of Michigan draws on the constructs of information process time and accuracy and suggests a relationship and trade-off, known as the speed-accuracy trade-off (SAT) (Swanson & Briggs 1969). Media synchronicity theory can predict InfoSec policy failure partly because the information used to define the policies and procedures at the higher levels of management is not related to the lower levels of the organisation. This creates 'broken telephone' communication. By the time information reaches the top management, it has lost its essence and depth (Dennis et al. 2008). We therefore propose the following:

H3: Time taken to process information will predict compliance with InfoSec policies.

In MST, individuals with shared mental models will use reason to encode and decode new messages faster (Dennis et al. 2008). Individual actions based on reason, can help support synchronicity, which is a shared pattern of co-ordinated behaviour among employees as they collaborate (Dennis et al. 2008). According to Burgemeestre, Hulstijn and Tan (2011), collaboration and compliance can be achieved 'by design'. This may be through instituting a rational system of controls consisting of information systems and procedures. Their work uses argumentation theory into the compliance domain and shows that value-based argumentation and reason are an important facet for compliance. We therefore propose the following:

H4: Reason for communicating (InfoSec policy) will predict compliance with InfoSec policies.

Media can influence user behaviour by making it easier for them to either interact or make it harder for them to interact. Media that fits well within the user's needs (media appropriateness) is more likely to be adopted and used. Positive past experiences and social norms can also affect the likelihood of that media being adopted (Dennis et al. 2008). We therefore propose the following:

H5: Media appropriateness will predict compliance with InfoSec policies.

Communication theory

Communication, espoused by psychologists in the psychology domain is central to human interaction and will consist of intrapersonal and interpersonal communication. Intrapersonal communication is an internal dialogue with self and consists of different subconscious reasoning processes that an individual takes on whilst thinking about

a specific subject. This includes contemplating alternatives, deciding between options, weighing up facts and determining how truthful the statement is. It also considers evaluating the intentions behind the actions of individuals, attitude, analysing, thinking, introspecting and self-talking (McQuail 2010). Interpersonal communication takes place when two individuals engage with each other. Formal and informal exchanges form part of interpersonal communication.

Communicating InfoSec policies will require two main players. The first player would be the person formulating and disseminating policy (sender) and the second player would be the person to receive and to comply with policy (receiver). The sender, in this case management may formulate an appropriate InfoSec policy by selecting words, gestures and mediums to compose the message. The encoding process can take the form of verbal, non-verbal or written language (Lunenburg 2010). Messages are carried through an appropriate medium such as telephonic, face-to-face, email or a written report depending on context. The evolution of technology has made email the most frequent and popular medium of choice in many organisations. For effectiveness, all components of communication must be interdependent and when there is a problem with one of these components, the whole communication process becomes flawed (Lunenburg 2010). We therefore propose the following:

H6: Communication media will predict compliance with InfoSec policies.

Media richness theory

Media richness theory drawn from the information systems discipline is rooted on the assumption that organisations process information in order to decrease the level of uncertainty and equivocality. According to Dennis and Kinney (1998) an ambiguous task may cause conflicting interpretation because people may lack the necessary information to process such a task (Dennis & Kinney 1998). In other words, the more InfoSec policies there are, the more uncertainty and equivocality these create and ultimately, this will create an impact on compliance. On the one hand, written media such as written InfoSec policies have been preferred for certain tasks that have clear messages. On the other hand, face to face InfoSec policies have been preferred for messages containing equivocality (Dennis & Kinney 1998). Media richness is hierarchical and will include four media groups, namely: (1) face-to-face, (2) telephone, (3) addressed documents, and (4) unaddressed documents (Daft, Lengel & Trevino 1987). Media richness theory postulates that information richness will influence how the message is interpreted, as this avoids ambiguity. We therefore propose the following:

H7: Non-conflicting interpretations will predict compliance with InfoSec policies.

Reducing uncertainty is an important aspect that is required when pieces of information is lacking. This can be addressed

by collecting more information in a less ambiguous environment. Communication can thus be managed by using less-rich media (Donabedian 2006). We therefore propose the following:

H8: Certainty will predict compliance with InfoSec policies.

It can be noted that richer media will be able to elicit immediate feedback, which can either be concurrent feedback or sequential feedback. Concurrent feedback usually takes place simultaneously with the communication of a message, whilst sequential feedback usually takes place when the receiver interrupts the sender to indicate understanding of a message (Kahai & Cooper 2003). We therefore propose the following:

H9: Feedback immediacy will predict compliance with InfoSec policies.

Personalisation is seen as using a technology and information in customised content aimed at matching individual needs and satisfaction and will require a personal focused approach (Hsu & Kulviwat 2006). The same can be said about any policy formulated that must be matched to individual and organisational needs for an effective compliance. We therefore propose the following:

H10: Personal focused (InfoSec policy) will predict compliance with InfoSec policies.

Theoretical framework

From the above literature review we were able to formulate the MPD framework from archetypes of communication theories and surrogates as shown in Figure 1 and to determine the strengths of each of these archetypes.

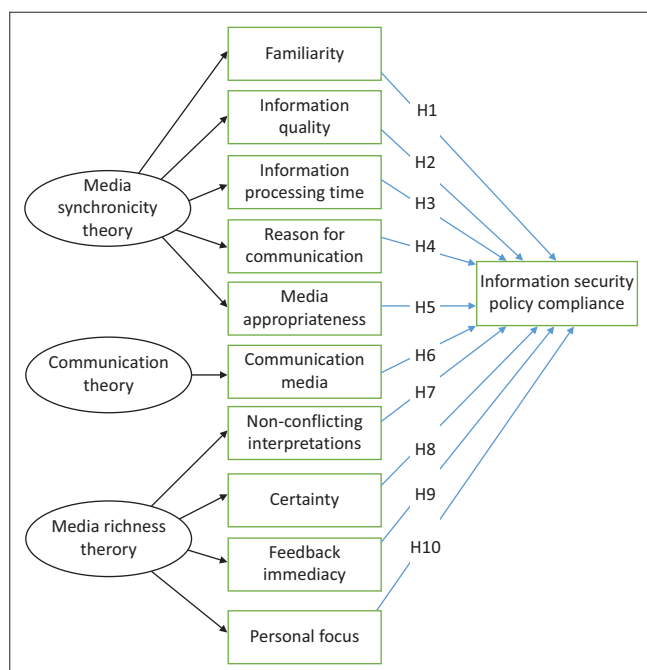


FIGURE 1: Miscellany of perception and determinism framework for communicating InfoSec policies.

Methodology

The study followed a quantitative approach to test the MPD framework, whilst using a probability sample of 100 individuals. The target sample comprised of employees working in organisations who had developed and communicated recent InfoSec policy documents to its employees. We used probability sampling because this approach was deemed suitable in covering an equal representation of the population (Pallant 2007). A closed-ended five point Likert-scale questionnaire was used as the primary data collection instrument. It contained constructs derived from communication, media synchronicity and media richness theories. A five point Likert scale was used to rate employee's perceptions, regarding how InfoSec policies were communicated and the strengths of the process leading to compliance or non-compliance. The questionnaires were sent for ethical clearance prior to distribution and upon receipt of ethical clearance, distributed to six different organisations operating in Johannesburg, South Africa. Data collected were anonymised and could not be traced back to a specific individual.

Ethical consideration

The research adhered to all ethical clearance procedures stipulated and approved by the School of Consumer Intelligence and Information Systems Ethics committee at the University of Johannesburg (2018SCiiS 01).

Data analysis

Statistical Package for the Social Sciences (SPSS), a computerised statistical analysis software was used for data analysis. The analysis enabled interpretation of results quantitatively, as well as presenting a logical flow of results. We noted instances where one respondent did not answer certain sections in the questionnaire (revealing academic qualifications) and this constituted missing data. We used SPSS frequency analysis to compute system missing data for each specific case, before further analysis was done. Upon examination, missing data did not constitute more than 1% of sample size, and we used SPSS factor procedure, pairwise deletion to exclude the variable that had a missing value (Norušis 2006). Table 2 shows Cronbach's alpha values elicited and reliability of data that was presented. This analysis takes cognisance of missing data. Cronbach's alpha

TABLE 2: Reliability analysis.

Factor item	Cronbach's alpha value	Number of items
Familiarity	0.852	4
Information quantity	0.758	2
Information process time	0.814	3
Reason for communication	0.776	4
Media appropriateness	0.657	2
Communication media	0.772	5
Non-conflicting interpretations	0.824	4
Certainty	0.784	3
Feedback immediacy	0.817	2
Personal focus	0.814	2

values greater than or equal to 0.9 suggests that internal consistency (correlation) is excellent. If the Cronbach's alpha value is less than or equal to 0.5, internal consistency (correlation) is very low and revising the items in the research instrument is recommended. Table 2 shows that familiarity, non-conflicting interpretations, information process time, feedback immediacy and personal focus have higher correlation values of above 0.8.

Descriptive statistics

Figure 2 describes the age of the participants. The majority of participants were between the ages of 25 and 34, which represented 64% of the sample.

Those aged between 18 and 24 represented 18% of the sample, whilst those aged between 35 and 44 represented 13% of the sample. The smallest group of participants were aged between 45 and 55 years old and this group represented 4% of the sample. Figure 3 describes the qualification levels of

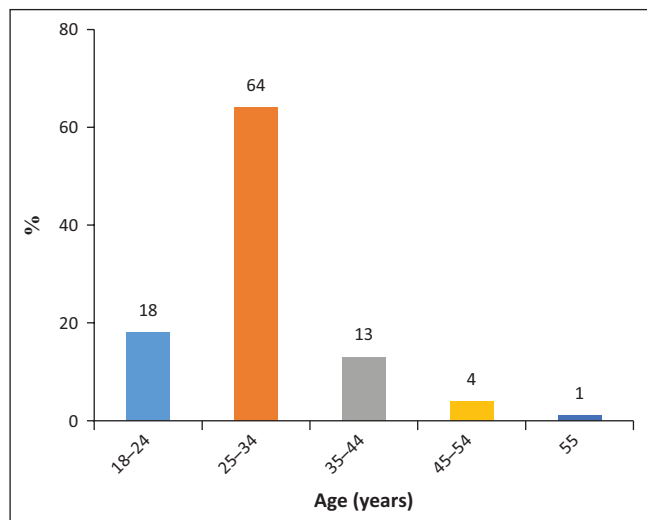


FIGURE 2: Age of participants.

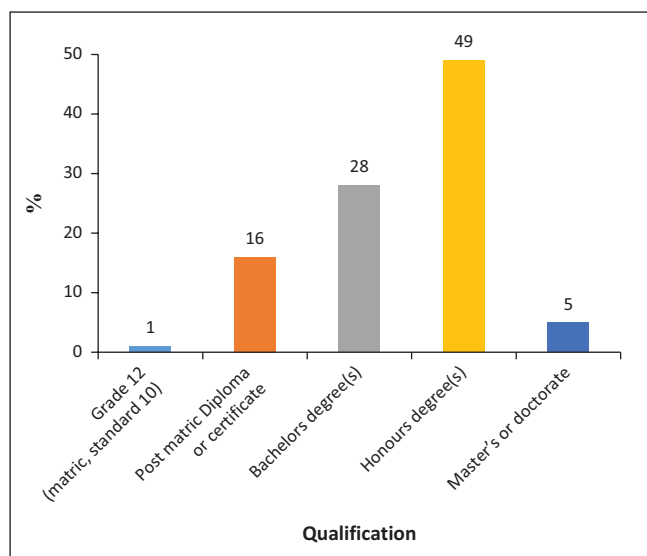


FIGURE 3: Participants' highest level of qualification.

participants and shows that 49% of those sampled held an honours degree, whilst 28%, held a baccalaureate degree. The less qualified of the sample included those who held a diploma, constituting 16% of the sample and those holding a matric certificate at only 1% of sample. The most qualified held masters or doctorate degree, and this represented 5% of the sample. A total of 1% of the respondents (missing data) did not disclose this information.

Importantly, the majority of those sampled in the study worked in an organisation that housed 1000 or more employees consisting of 75% of sample. This is shown in Figure 4.

A total of 13% of respondents worked in an organisation that housed the number of employees ranging between 101 and 500. Less than 7% of those sampled worked for an organisation with less than 500 employees and 4% worked for an organisation with 1 and 49 employees. Only 1% of those sampled worked in an organisation housing 50 and 100 employees.

Factor analysis

Ten key constructs drawn from the MDP framework, namely familiarity, information quantity, information process time, reason for communication, media appropriateness, communication media, non-conflicting interpretations, certainty, feedback immediacy and personal focus that were proposed to predict compliance of InfoSec were considered. We carried out a factor analysis to reduce the underlying variables associated with each of these constructs. We used SPSS, factor analysis (principal component analysis) for this purpose. We used Bartlett's test of sphericity to test construct validity. In addition, in order to analyse the strength existing between variables, Kaiser-Mayer-Olkin's (KMO) measure of sampling adequacy was used. Kaiser-Mayer-Olkin's results were used to determine whether factor analysis would be a good method to use for dimension reduction and multicollinearity of values ranging between 0 and 1. Our values were above 0.5 and close to 1.0 indicating that a factor analysis would be useful. The KMO values are presented in Table 3.

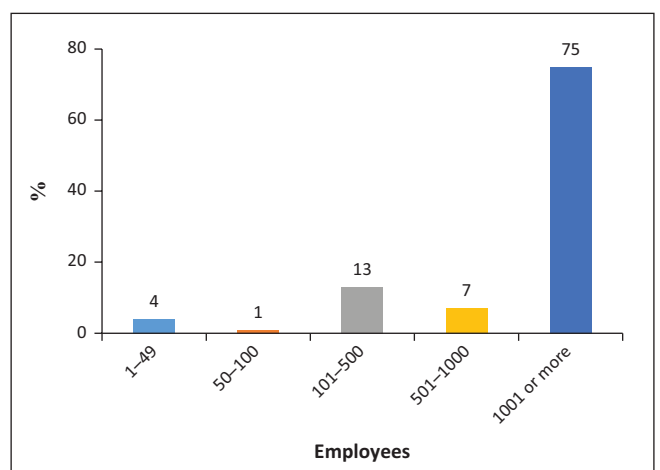


FIGURE 4: Number of employees in sampled organisations.

TABLE 3: Kaiser–Mayer–Olkin and Bartlett’s test.

Test	Variable	Media Synchronicity: Familiarity Information quantity Information process time Reason for communication Media appropriateness	Communication: Communication media	Media Richness: Non-conflicting interpretations Certainty Feedback immediacy Personal focus
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.	-	0.571	0.728	0.706
Bartlett’s Test of Sphericity	Approximate chi-square	139.251	77.598	98.440
	<i>df</i>	10	15	10
	Sig.	0.000	0.000	0.000

df, degrees of freedom; Sig., significance.

TABLE 4: Extract table of factor analysis for media synchronicity.

Factor	Initial eigenvalues		
	Total	Variance (%)	Cumulative (%)
1	4.781	23.904	23.904
2	3.061	15.305	39.209
3	2.499	12.495	51.704
4	1.539	7.694	59.398
5	1.187	5.934	65.332
6	1.069	5.343	70.675
7	0.876	4.379	75.054
8	0.731	3.654	78.708
9	0.718	3.590	82.297
10	0.560	2.802	85.099

TABLE 5: Extract table of factor analysis for media richness.

Factor	Initial eigenvalues		
	Total	Variance (%)	Cumulative (%)
1	5.395	31.736	31.736
2	2.606	15.331	47.067
3	1.725	10.144	57.212
4	1.259	7.405	64.617
5	1.001	5.887	70.504
6	0.812	4.775	75.279
7	0.736	4.329	79.608
8	0.617	3.630	83.238
9	0.561	3.299	86.538
10	0.493	2.902	89.440

From the KMO results indicating that factor analysis would be useful, we carried out a factor analysis and rotated components for better interpretation and the elimination of ambiguity (Pallant 2007) as indicated by Table 4 and Table 5. Factor rotation’s main purpose is to create a simplified structure that enables all items to load based on a minimal number of factors (Yong & Pearce 2013). The results of factor analysis were used to measure the suitability of the data and of sampling adequacy for variables identified within the theoretical model.

Component extraction and factor loadings

Media synchronicity

Six factors were extracted. These six factors had an eigenvalues greater than one and together, they accounted for 71% of the variability in the original variables.

Communication

We did not carry out a factor analysis for this construct and used all five items for explaining the single item *communication media*. Using SPSS, we transformed these into a single factor by computing average means.

Media richness

Only five factors having eigenvalues greater than one were extracted, and together these accounted for 71% of the variability in the original variables.

Regression

A multiple regression analysis that describes the relationship and strength between the dependent variable, compliance of InfoSec policies, and the 10 independent variables under study was carried out. The purpose was to estimate the coefficient of the 10 independent variables, on the variable compliance of InfoSec policies. The results of the regression analysis are shown in Table 6.

Discussion

Based on the outcomes of the tests, the overall significance of the research model was justified. However, five of the following hypotheses, namely *familiarity*, *information quality*, *information process time*, *communication media* and *certainty* were rejected because of their insignificant values (where $p < 0.0005$), whilst those propositions that were accepted have a bearing on compliance as presented in Figure 5. It is important to note that although the ‘reject’ lexicon has been used, this simply means that the results were non-significant with no way to determine if these five could predict compliance (Ghauri, Grønhaug & Strange 2020).

From the linear regression analysis communication archetypes of *reasons for communication*, *media appropriateness*, *non-conflicting interpretations*, *feedback immediacy* and *personal focus* tended to significantly predict compliance with InfoSec policies as opposed to other archetypes that were disproved in the MPD model. We address each of these variables as follows: *Reason for communication* was statistically significant towards predicting InfoSec policy compliance, beta = 0.306 and significant value < 0.5. When organisations re-emphasise the reason why certain policies are important, employees are more likely to comply. Importantly, regarding *media appropriateness*, (beta = 0.280 and significant value < 0.5) when the choice of media of communication is deemed appropriate by employees, the security compliance is predictably higher and when the choice of media is inappropriate chances of non-compliance are heightened. This study confirms the finding of other studies carried out that give preference and significance to explicit forms of communication such as email (Fonseca & Normann 2012). With regard to the variable *non-conflicting*

TABLE 6: Multiple regression results.

Model	Unstandardised Coefficients		Standardised Coefficients: Beta	t	Significance	Correlations		
	B	Standard error				Zero-order	Partial	Part
1. Familiarity	0.259	0.114	0.224	2.271	0.025	0.224	0.224	0.224
2. Information quality	0.068	0.086	0.079	0.787	0.433	0.079	0.079	0.079
3. Information process time	0.066	0.090	0.074	0.735	0.464	0.074	0.074	0.074
4. Reason for communication	0.373	0.117	0.306	3.182	0.002	0.306	0.306	0.306
5. Media appropriateness	0.250	0.087	0.280	2.889	0.005	0.280	0.280	0.280
6. Communication media	0.222	0.087	0.251	2.571	0.012	0.251	0.251	0.251
7. Non-conflicting interpretations	0.560	0.095	0.510	5.873	0.000	0.510	0.510	0.510
8. Certainty	0.096	0.096	0.100	0.998	0.321	0.100	0.100	0.100
9. Feedback immediacy	0.248	0.083	0.288	2.978	0.004	0.288	0.288	0.288
10. Personal focus	0.483	0.088	0.486	5.512	0.000	0.486	0.486	0.486

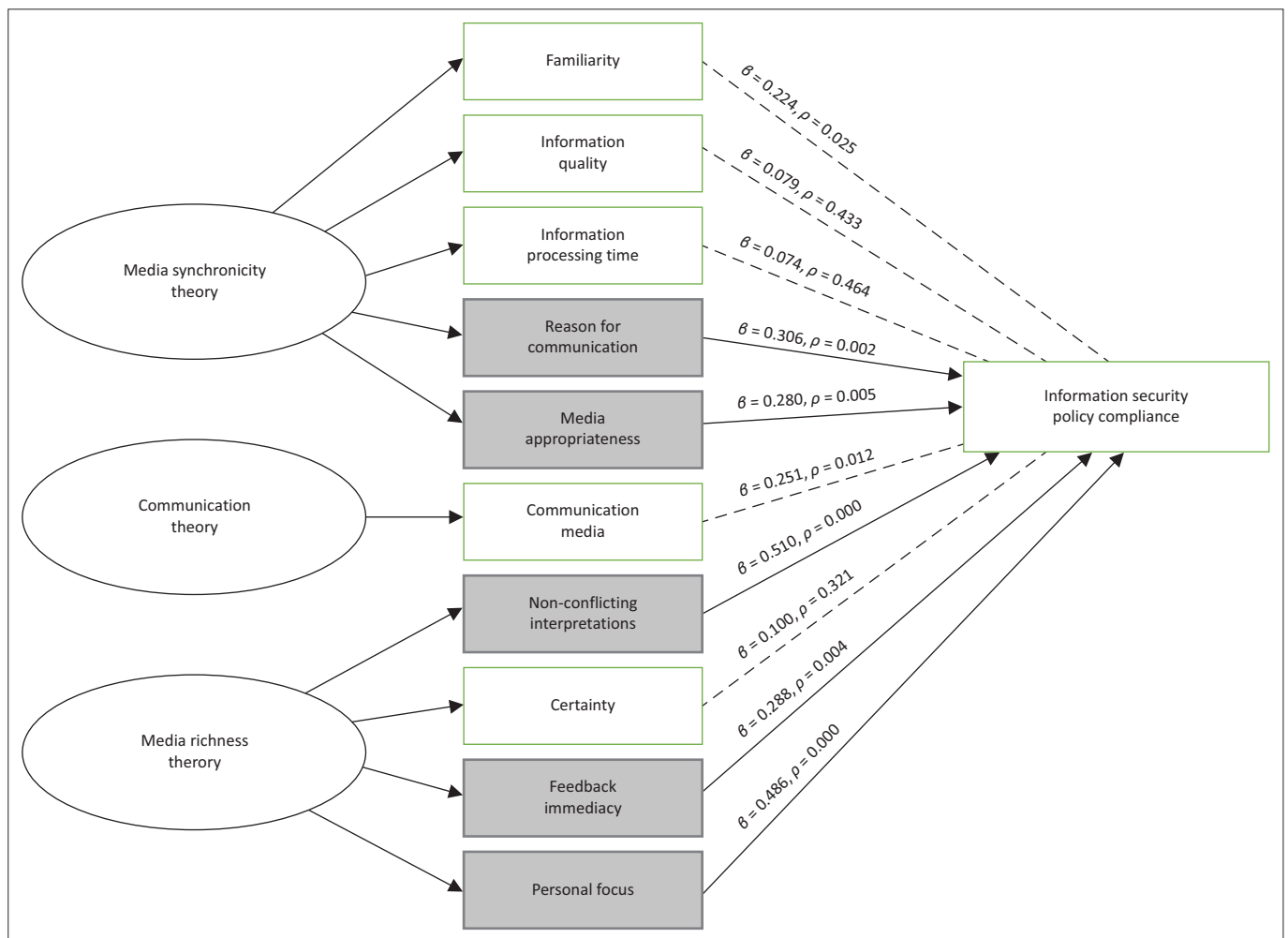


FIGURE 5: Miscellany of perception and determinism predicting compliance.

interpretations, (beta = 0.306 and significant value < 0.5.) data results suggest that if policies are ambiguous, then this tends to predict non-compliance. If InfoSec policies are non-conflicting and unambiguous, then this tends to predict compliance. According to Buthelezi, Van Der Poll and Ochola (2016), InfoSec policies may often not be followed nor complied with because of the very nature of the policy documents themselves, which may lend themselves to misinterpretation. Indeed ambiguity in wordings in such documents makes it hard for users to comply. This work presents a similar viewpoint from those observations and shows ambiguity will limit compliance. *Feedback immediacy* (where beta = 0.288 and

significant value < 0.5) was statistically significant and also tended to predict security compliance. Indeed, when the media selected enables real-time or immediate feedback from both sender and receiver, the InfoSec policy being sent is more likely to be complied with (Keil & Johnson 2002). Significantly, studies have drawn a link between performance and communication frequency, when feedback is received repeatedly (McLarnon et al. 2019) and this study confirms this as well. Our findings and therefore proposition is that these five variables will ameliorate InfoSec policy compliance more intensely if keen attention is given to these by management and practitioners.

Contribution

The MPD framework developed in this work, offers new communication predilections that can shape InfoSec policy compliance in ways not considered before in InfoSec literature. These communication predications are characterised by *non-conflicting interpretations, reasons for communication, media appropriateness, feedback immediacy and personal focus*. The MPD framework compels InfoSec practitioners to understand communication much more deeply and to leverage the medium and message in order to ameliorate InfoSec policy compliance.

Implications of study

InfoSec practitioners in South Africa and those in management may find the MPD framework useful in providing actionable insights into managing how InfoSec policies should be communicated in order to inspire high compliance. As we have shown, compliance with InfoSec policies is necessary to avoid business risk. The findings of this study can be broadly generalised and transferable to contexts outside of South Africa. In terms of a theoretical implication, the research advances InfoSec literature by adapting the MPD model as integral to the development and communication of policies. The MPD model is pertinent as it aggregates theories of communication from a number of academic disciplines and underpinnings not considered before, thereby improving our understanding on how we communicate InfoSec policies.

Conclusion

InfoSec policies are designed primarily to ensure that users of organisations' information assets abide by, and follow, specified prescriptions in order to protect information assets from threats. Notably, users have been shown to be less compliant with InfoSec policies thus compelling a need to investigate why this is so. Following through a literature review and focusing on how policies are communicated to users whom literature has identified as threats, this research was undertaken to present a communication model that could predict InfoSec policy compliance. The research aggregates theories of communication and develops the MPD framework, which was considered pertinent as it draws insights from a number of academic disciplines and underpinnings not considered before. It is through the MPD framework that our understanding regarding how we communicate InfoSec policies is improved. The inferences of the MPD framework show that there is a strong positive relationship between InfoSec compliance (and non-compliance) that is shaped by *reasons for communication, media appropriateness, non-conflicting interpretations, feedback immediacy and personal focus*. These five constructs predict 61.3% of InfoSec compliance. The remaining five constructs, namely *familiarity, information quality, information processing time, communication media and certainty* were tested and found to be weak predictors or could not predict compliance. In light of these findings, this work has made several suggestions to organisations

such as the need to reemphasise the reason why certain policies are important, availing immediate feedback when there are signs non-compliance is imminent and importantly carefully determining the appropriate media to use when communicating InfoSec policies. This work opens up possibilities for important future research where the MPD model needs to be tested in multiple settings as communication of InfoSec policies may vary under different settings. The MPD framework would have gone unnoticed without this empirical initiative.

Acknowledgements

Competing interests

The authors have declared that no competing interests exist.

Authors' contributions

All authors contributed equally to this work.

Funding information

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

Data availability statement

The authors confirm that the data supporting the findings of this study are available within the article.

Disclaimer

The views and opinions expressed in this article are those of the author and do not necessarily reflect the official policy or position of any affiliated agency of the authors.

References

- Adriaanse, L.S. & Rensleigh, C., 2017a, 'E-visibility to enhance knowledge sharing', in *Africa Research Group Conference*, Mauritius, August 29–31, 2017.
- Adriaanse, L.S. & Rensleigh, C., 2017b, 'E-visibility of environmental science researchers at the University of South Africa', *South African Journal of Libraries and Information Science* 83(2), 30–41. <https://doi.org/10.7553/83-2-1636>
- Aurigemma, S., 2013, *From the weakest link to the best defense: Exploring the factors that affect employee intention to comply with information security policies*, ProQuest LLC, Manoa, HI.
- Borena, B., Belanger, F. & Dedefa, D.E., 2015, 'Information privacy protection practices in Africa: A review through the lens of critical social theory', in *48th Hawaii International Conference on System Sciences*, HICSS 2015, Kauai, Hawaii, USA, January 05–08, 2015. IEEE Computer Society 2015, 3490–3497. <https://doi.org/10.1109/HICSS.2015.420>
- Burgemeestre, B., Hulstijn, J. & Tan, Y.H., 2011, 'Value-based argumentation for justifying compliance', *Artificial Intelligence and Law* 19(2–3), 149. <https://doi.org/10.1007/s10506-011-9113-4>
- Buthelezi, M.P., Van der Poll, J.A. & Ochola, E.O., 2016, 'Ambiguity as a barrier to information security policy compliance: A content analysis', in *Proceedings of the International Conference on Computational Science and Computational Intelligence* (CSCI), December 15–17, 2016, pp. 1360–1367, IEEE, Las Vegas, NV.
- Cannon, J.C. & Byers, M., 2006, 'Compliance deconstructed', *Queue*, 4(7), 30–37. <https://doi.org/10.1145/1160434.1160449>
- Chen, C.C. & Chang, Y.C., 2018, 'What drives purchase intention on Airbnb? Perspectives of consumer reviews, information quality, and media richness', *Telematics and Informatics* 35(5), 1512–1523. <https://doi.org/10.1016/j.tele.2018.03.019>
- Chen, P.S.T., Srinivasan, K.K. & Mahmassani, H.S., 1999, 'Effect of information quality on compliance behavior of commuters under real-time traffic information', *Transportation Research Record* 1676(1), 53–60. <https://doi.org/10.3141/2162-07>
- D'Arcy, J., Herath, T. & Shoss, M.K., 2014, 'Understanding employee responses to stressful information security requirements: A coping perspective', *Journal of Management Information Systems* 31(2), 285–318. <https://doi.org/10.2753/MIS0742-1222310210>

- 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>
- Daft, R.L., Lengel, R.H. & Trevino, L.K., 1987, 'Message equivocality, media selection, and manager performance: Implications for information systems', *MIS Quarterly* 11(3), 355–366. <https://doi.org/10.2307/248682>
- Dennis, A.R. & Kinney, S.T., 1998, 'Testing media richness theory in the new media: The effects of cues, feedback, and task equivocality', *Information Systems Research* 9(3), 219–301. <https://doi.org/10.1287/isre.9.3.256>
- Dennis, A.R., Fuller, R.M. & Valacich, J.S., 2008, 'Media, tasks, and communication processes: A theory of media synchronicity', *MIS Quarterly* 32(3), 575–600. <https://doi.org/10.2307/25148857>
- Donabedian, B., 2006, 'Optimization and its alternative in media choice: A model of reliance on social-influence processes', *Information Society* 22(3), 121–135. <https://doi.org/10.1080/01972240600677771>
- Du Plessis, T. & Gulwa, M., 2016, 'Developing a competitive intelligence strategy framework supporting the competitive intelligence needs of a financial institution's decision makers', *South African Journal of Information Management* 18(2), 1–8. <https://doi.org/10.4102/sajim.v18i2.726>
- Eloff, J.H.P. & Eloff, M.M., 2005, 'Information security architecture', *Computer Fraud & Security* 2005(11), 10–16. [https://doi.org/10.1016/S1361-3723\(05\)70275-X](https://doi.org/10.1016/S1361-3723(05)70275-X)
- Fitzpatrick, W.M. & Burke, D.R., 2003, 'Competitive intelligence, corporate security and the virtual organization', *Journal of Competitiveness Studies* 11(1), 20–30.
- Fonseca, M.A. & Normann, H.T., 2012, 'Explicit vs. tacit collusion – The impact of communication in oligopoly experiments', *European Economic Review* 56(8), 1759–1772. <https://doi.org/10.1016/j.euroecorev.2012.09.002>
- Frasier, L.L., Quamme, S.R.P., Ma, Y., Wiegmann, D., Leverson, G., DuGoff, E.H. et al., 2019, 'Familiarity and communication in the operating room', *Journal of Surgical Research* 235, 395–403. <https://doi.org/10.1016/j.jss.2018.09.079>
- Ghauri, P., Grønhaug, K. & Strange, R., 2020, *Research methods in business studies*, Cambridge University Press, Cambridge.
- Herath, T. & Rao, H., 2009, 'Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness', *Decision Support Systems* 47(2), 154–165. <https://doi.org/10.1016/j.dss.2009.02.005>
- Hsu, H.S. & Kulviwat, S., 2006, 'An integrative framework of technology acceptance model and personalisation in mobile commerce', *International Journal of Technology Marketing* 1(4), 393–410. <https://doi.org/10.1504/IJTMKT.2006.010734>
- Hu, Q., Xu, Z., Dinev, T., Ling, H., 2011, 'Does deterrence work in reducing information security policy abuse by employees?', *Communications of the ACM* 54(6), 54–60. <https://doi.org/10.1145/1953122.1953142>
- Isaak, J. & Hanna, M.J., 2018, 'User data privacy: Facebook, Cambridge analytica, and privacy protection', *Computer* 51(8), 56–59. <https://doi.org/10.1109/MC.2018.3191268>
- Kahai, S.S. & Cooper, R.B., 2003, 'Exploring the core concepts of media richness theory: The impact of cue multiplicity and feedback immediacy on decision quality', *Journal of Management Information Systems* 20(1), 263–299. <https://doi.org/10.1080/07421222.2003.11045754>
- Kandeh, A.T., Botha, R.A. & Futcher, L.A., 2018, 'Enforcement of the Protection of Personal Information (POPI) Act: Perspective of data management professionals', *South African Journal of Information Management* 20(1), 1–9.
- Keil, M. & Johnson, R.D., 2002, 'Feedback channels: Using social presence theory to compare voice mail to e-mail', *Journal of Information Systems Education* 13(4), 4.
- Kirlappos, I., Parkin, S. & Sasse, M.A., 2014, *Learning from 'Shadow Security': Why understanding non-compliance provides the basis for effective security*, OpenAIRE, UK. <http://doi.org/10.14722/usec.2014.23007>
- Lowry, P.B. & Moody, G.D., 2015, 'Proposing the control reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies', *Information Systems Journal* 25(5), 433–463. <https://doi.org/10.1111/isj.12043>
- Lunenburg, F., 2010, 'Communication: The process, barriers, and improving effectiveness', *Schooling* 1(1), 1–11.
- McLarnon, M.J., O'Neill, T.A., Taras, V., Law, D., Donia, M.B. & Steel, P., 2019, 'Global virtual team communication, coordination, and performance across three peer feedback strategies', *Canadian Journal of Behavioural Science / Revue canadienne des sciences du comportement* 51(4), 207–218. <https://doi.org/10.1037/cbs000135>
- McQuail, D., 2010, *McQuail's mass communication theory*, Sage, Newbury Park, CA.
- Mthembu, M. & Du Plessis, T., 2018, 'Maturity mapping for continuous improvement: A case study of a revenue services institution', *South African Journal of Economic and Management Sciences* 21(1), 1–10. <https://doi.org/10.4102/sajems.v21i1.2044>
- Musarurwa, A. & Flowerday, S., 2018, 'The BYOD information security challenge for CIOs', in *Proceedings of the 12th International Symposium on Human Aspects of Information Security & Assurance*, August 29–31, 2018, p. 246, Dundee, Scotland.
- Niemand, C.J. & Mearns, M., 2020, 'Elements of a flexible information architecture: A South African perspective', *South African Journal of Information Management* 22(1), 1–7. <https://doi.org/10.4102/sajim.v22i1.1007>
- Norušis, M.J., 2006, *SPSS 14.0 guide to data analysis*, Prentice hall, Upper Saddle River, NJ.
- Odine, M., 2015, 'Communication problems in management', *Journal of Emerging Issues in Economics, Finance and Banking (JEIFEB)* 4(2), 1615–1630.
- Pallant, J., 2007, 'SPSS survival manual', in J. Pallant (ed.), *SPSS survival manual*, p. 146, Open University Press, Maidenhead.
- Posey, C., Roberts, T.L., Lowry, P.B., 2015, 'The impact of organizational commitment on insiders' motivation to protect organizational information assets', *Journal of Management Information Systems* 32(4), 179–214. <https://doi.org/10.1080/07421222.2015.1138374>
- Poulet, Y., 2006, 'EU data protection policy, the directive 95/46/EC: Ten years after', *Computer Law & Security Report* 2(2), 206–217. <https://doi.org/10.1016/j.clsr.2006.03.004>
- Puhakainen, P. & Siponen, M., 2010, 'Improving employees' compliance through information systems security training: An action research study', *MIS Quarterly* 34(4), 757–778. <https://doi.org/10.2307/25750704>
- Sanders, J. & Patterson, D., 2019, *Facebook data privacy scandal: A cheat sheet*, Tech Republic, viewed 14 May 2020, from <https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/>
- Sharma, S. & Warkentin, M., 2018, 'Do I really belong?: Impact of employment status on information security policy compliance', *Computers & Security* 87, 101397. <https://doi.org/10.1016/j.cose.2018.09.005>
- Siponen, M., Mahmood, A. & Pahlila, S., 2009, 'Are employees putting your company at risk by not following information security policies?', *Communication of the ACM* 52(12), 145–147. <https://doi.org/10.1145/1610252.1610289>
- Susmilch, C., 2019, *Let's talk – communication strategies that engage employees and improve compliance*, Sumerra, viewed 30 May from <https://www.sumerra.com/lets-talk-communication-strategies-that-engage-employees-and-improve-compliance/>
- Swanson, J.M. & Briggs, G.E., 1969, 'Information processing as a function of speed versus accuracy', *Journal of Experimental Psychology* 81(2), 223–229. <https://doi.org/10.1037/h0027774>
- Tikkinen-Piri, C., Rohunen, A. & Markkula, J., 2018, 'EU general data protection regulation: Changes and implications for personal data collecting companies', *Computer Law & Security Review* 34(1), 134–153. <https://doi.org/10.1016/j.clsr.2017.05.015>
- Vance, A. & Siponen, M.T., 2012, 'IS security policy violations: A rational choice perspective', *Journal of Organizational and End User Computing (JOEUC)* 24(1), 21–41. <https://doi.org/10.4018/joeuc.2012010102>
- Whitman, M.E., 2003, 'Enemy at the gate: Threats to information security', *Communications of the ACM* 46(8), 91–95. <https://doi.org/10.1145/859670.859675>
- Williams, P., 2001, 'Information security governance', *Information Security Technical Report* 6(3), 60–70. [https://doi.org/10.1016/S1363-4127\(01\)00309-0](https://doi.org/10.1016/S1363-4127(01)00309-0)
- Yong, A. & Pearce, S., 2013, 'A beginner's guide to factor analysis: Focusing on exploratory factor analysis', *Tutorials in Quantitative Methods for Psychology* 9(2), 79–94. <https://doi.org/10.20982/tqmp.09.2.p079>