Information Security Policy Compliance: A Broad-based Literature Review and a Theoretical Framework

Erick O. Otieno
University of Nairobi

Andrew M. Kahonge
University of Nairobi

Agnes N. Wausi
University of Nairobi

ABSTRACT
Despite a plethora of studies in the field of information security and a vast pool of measures to mitigate insider threats, risks still exist especially with the challenging environment information security practitioners experience due to noncompliance with information security policies. Employee's noncompliance is made even worse since third parties contracted by organizations cannot guarantee that whilst handling their respective information assets, the respective information security managers of the said third party entities will not guarantee information security policy compliance on the other side. Therefore, getting a solution that assists the information security managers handle the "Phantom insiders" in the same way they mitigate internal insider would be ideal. This review steps in to this gap and reviews what has been covered and what still needs to be done, then proposes a future framework for researchers alongside other recommendations for practitioners. We add a dimension to the insider threat meaning to broaden the scope to include employees and stakeholders of third-party entities. We define four thematic areas that can inform future research by grounding our analysis in extant information security policy compliance literature within a span of 15year. We finally propose a framework that will work as a foundation for future information security policy compliance research and practice.

Keywords
Information Security Policy Compliance, Theoretical Concept, Insider Threats, Insiders in Cloud Computing

1. INTRODUCTION
While there is still differing opinion among scholars on whether insider threats should include external contractors having access to organizational assets, there is a consensus on insider threats in general being the most challenging information security attack vector that has proven to be difficult to deal with in organizations. Insiders have been quoted to contribute to about 27% of all cyber-crime incidents in a recent survey while the same survey indicated that 30% of those who were interviewed believed that insiders inflicted more damage as compared to attackers from outside [1]. Another survey by [2] which investigated economic crime noted that 29% of the cases were due to internal fraudsters. Similar to the report by Trzeciak in terms of the number quoted, electronic attacks were believed to be perpetrated by insiders while those who believed that that insiders caused more damage to organizational information systems than outsider attacks stood at 45% [3]. With regards to outsourced services and threats from cloud environment, a report attributed to McAffee indicated a significant increase of sensitive data shared across Cloud environment standing at 21% up by 17% over past two years alone [4]. The same report points to the fact that organizations experience at least 1 compromised cloud accounts per month which stands at 80% out of all organizations while 90% of organizations have had their cloud credentials stolen for malicious purposes such as the culprits selling them to the dark web. These are just a few statistics and there could be more with regards to cloud.

All the statistics above do not only show how serious information security as an area of inquiry is important but can be construed as an indicator that holistic approach to ensuring information security policy compliance is achieved both within the organization and within the contracting partners and stakeholders having access to organizational information systems assets.

1.1 Information Security Policy Compliance Reviews Overview
One closely related review related to theories that explain information security policy compliance behaviour was that done by [5]. The authors sought to explore relatively used theories that explained security related awareness and behavioural aspects of employees in literature. However, the unit of analysis under the review study seemed to have focused more on individual behaviour as opposed to our review that broadens its scope to include extant works that have covered both individuals and organization as units of analyses.

A look at the review by [6] reveals a much more robust coverage of information security especially with the added dimension of negligent and malicious insiders. This additional dimension about insiders however did not address or did not give a conclusive distinction between insiders that are within the control of the organization and the insiders operating remotely within or remotely by virtue of being employees or third parties of contracted entities by the organizations in question. The authors also very elaborately discussed the Environmental countermeasures such as social measures that information systems IS managers apply in a bid to deter those who would think of not complying with information security policies or as an encouragement tool towards compliance with the policies [6]. Bringing in the organizational culture context would bring a broader dimension and promote the consideration of other antecedents that encourage compliance and discourage noncompliant behaviour especially for new members of the organization.

One other review by [7] discussed at length the relationships existing among constructs that contribute in one way or another to information security policy compliance in organization by individuals. The authors contributed to the body of knowledge through the extension of prior descriptive reviews of the security policy literature [7]. The epitome of their work resulted in developing a robust research framework that outlined security policies influencers and consequences. The resultant work by [7] can indeed be built upon by adding a new dimension of insiders emerging from third party entities

that have access to organizational information systems assets and services as already discussed above.

1.2 Review Questions (RQ)

RQ1: What are the constructs influencing the information security policy compliance existing in extant literature?

RQ2: What are the theoretical directions in information security policy compliance studies?

RQ3: What theoretical framework can be developed from the review outcome?

1.3 Review Objectives (RO)

RO1: Explore the constructs as applied in information security policy compliance studies in extant literature.

RO2: Identify theoretical thematic outcomes from the resulting constructs in the exploration.

RO3: Develop a refined theoretical framework for future consideration by researcher and practitioners.

1.4 Insider Threat Expanded Taxonomy

In order to address the review questions, we considered expanding the insider taxonomy for our review to be as wide as possible in covering all aspects of insider threats and thereby ensuring that the contribution of this review is helpful to both future researchers and practitioners. We proposed an insider taxonomy that adds a dimension based on the source of insider threat relative to the organisation that is outsourcing its information systems assets such as those in the cloud or outsourcing of services. The motivation for this taxonomic dimension is derived from fact that existing taxonomies have not addressed at length the aspects of source of these insider threats even though robust taxonomies do exists such as taxonomies by [8] [6]. While [8] covered the taxonomies of insiders based on levels of threats with regards to different cloud environment, such as whether the insiders were in the public, private or communal cloud, their classification differed from that of [6] who broadly categorized insiders as malicious and non-malicious against the willingness to comply and ability to protect or not protect information assets matrix. Our proposed taxonomy builds on these two latest taxonomies and introduces the dimension of the source of insider threats. As illustrated in our proposed taxonomy in Fig 1, this review will base its thematic components in relation to source of insiders and the type of insiders and explore how extant literature has covered the respective information security policy compliance in various setting. It is our submission that the taxonomy clarifies the constructs and the relationships existing between compliance predictors and policy compliance.

2. METHODOLOGY

We considered several approaches suggested by Webster and Watson to come up with the review strategy which looks at the concepts and units of analysis in terms of analysis of the reviewed literature [9]. In order to assist in developing a proper synthesis of literature, adoption of concept-centric in any review is highly recommended [9] and [10].

As noted by [11], there exist several review types that we also considered. The review types can be one of: theoretical review type, narrative review type, meta-analysis review type, descriptive review type, hybrid review type critical and scoping review type [11]. The same concept of classification can be found in [10] where the author identifies several categories of review [10].

As such, our review falls in the explanatory category of the literature review as explained by [10]. We adopt [10] views on what review articles should achieve and how it should achieve the objectives by generating concept-centric developed in terms of: (1) what influences the organizational enforcement of information policy compliance among its employees; (2) what influences organizations to force employees of third party entities such as employees in the outsourcing company

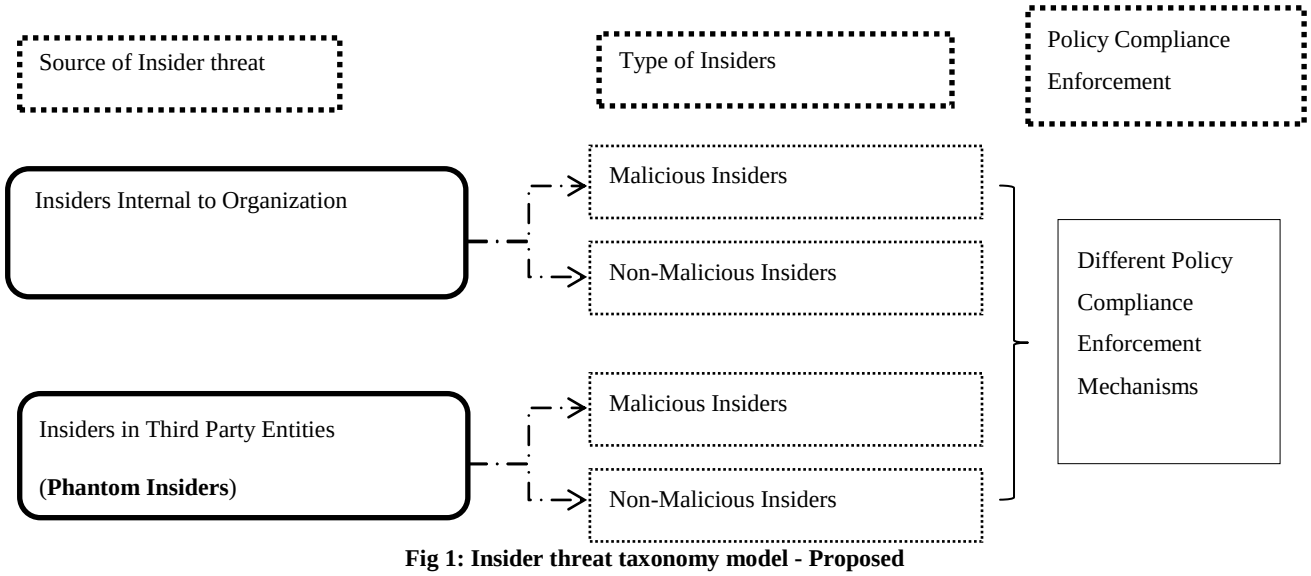

Fig 1: Insider threat taxonomy model - Proposed

or cloud service providers to comply with information security policies; (3) what influences individual employees to comply with information security policies in an organization; and (4) what technical related factors influences the compliance with information security policies by employees in an organization.

2.1 Review Boundaries

The sampling frame that we considered was a fifteen-year timeframe starting from 2004 to 2018 covering articles of all methodological approach and different philosophical approach. The decision not to set any boundary with regards

to methodology and philosophy is motivated by [10] in which the author highlights the interdisciplinary nature of information system studies. Papers that were excluded included but not limited to those that covered information security at application level especially if they did not include in part or in full aspects of information security policy compliance.

2.2 Literature Search and Selection Criteria

We consulted the Journal Quality List [12] as our first step in journal list selection to identify relevant literature to review that focuses in Information Systems Management and to some extent Knowledge Management. We compared the listings in the Journal Quality List with the top journal ranking platforms such as *Schimago Journal Database listings* and *Australian Business Deans Council listings* to verify and validate the consolidated listing of Journal Quality List. To ensure inclusivity and broad-based coverage, we searched all journals regardless of the *Journal* ranking with regards to top tier or lower tier. The key words that we considered included, "Cloud Insider Threat Mitigation", "Information Security Policy Compliance", "Information Security Policy Management in Organizations", "Information Security Compliance", "Theories in Information Security Policy Compliance research", "Constructs in Information Security Policy Compliance studies" and "Predictors in Information Systems Security Policy studies". A total of **45** articles were systematically identified and a selection of **28** articles from a diverse source of publishers made for actual review based on the respective article's area of inquiry.

2.3 Literature Review on Information Security Policy Compliance Behavior

From the expounded scope of insiders as depicted in Fig 1, we reviewed the literature on information security policy compliance from a different dimension and developed conceptual themes around the antecedents that guided on how we grouped the antecedents of information security policy compliance by employees. We considered the groupings of antecedents based on whether the measures were internal to the organization or external to the organization as shown in Fig 2.

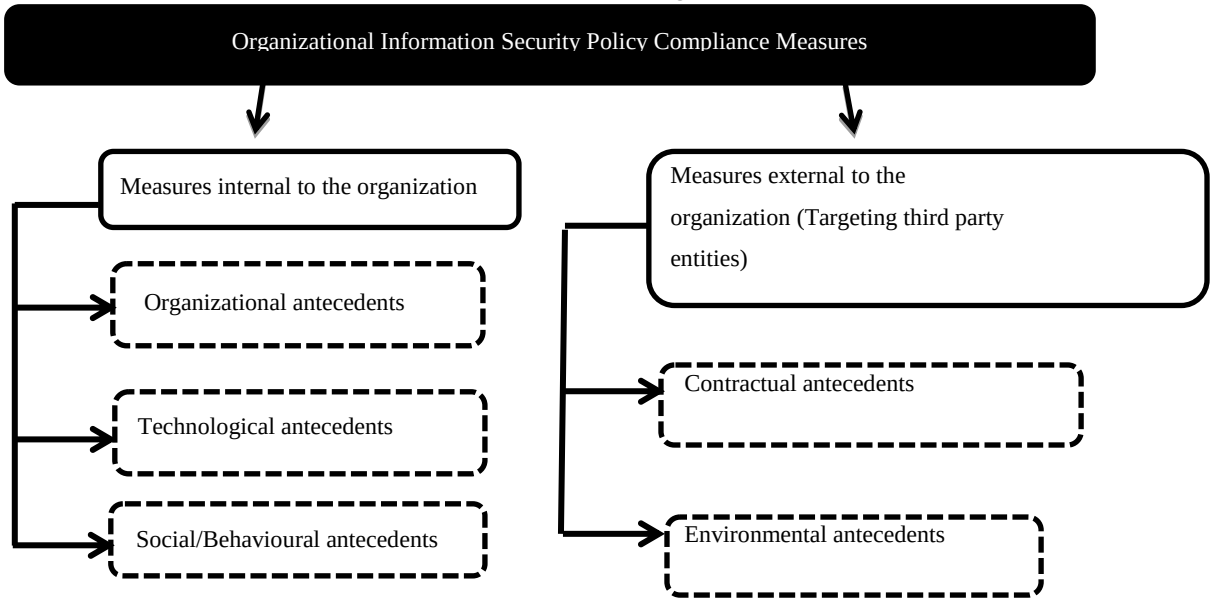

Fig 2: Conceptual illustration of key thematic concepts to be considered in this review

3. LITERATURE ANALYSIS RESULT

Results indicated a skewed trend with regards to how antecedents were applied in extant literature. As seen in Table 1, antecedents that fell within the social / behavioural level of antecedents amounted to 52 in count. This accounted for 57% of all antecedents that we analysed from extant literature. Antecedents that fell within the scope of Organizational level applicability, totalled to 20 in count which amounted to 22% of all antecedents. About technical antecedents, we analysed and only found 1 article that addressed the technological related antecedent namely Technology, Organization and Environment (TOE). This accounted for only 1%. In summary, the antecedents that could be related to third party measures to enhance compliance emerged at 20% which was 18 in total. The result shows that a lot of studies have concentrated on social behavioural aspects of information security compliance with studies focusing very minimally on technological factors that influence information security policy compliance behaviour.

Table 1. Tabulated synthesised results indicating broader antecedents' categories and their frequencies

		Antecedents under review categorization	Identified Antecedent by count	Frequency by (%)
Information security policy compliance issues covered in	Antecedents /Predictors internal to the organizational information security	Social / behavioural level applicability	52	57%
		Organizationa	20	22%

relation to our thematic concept	policy compliance	l level applicability		
		Technological level applicability	1	1%
	Antecedents /Predictors external to the organizational information security policy compliance	Third Party Contractual Framework Applicability	18	20%

4. DISCUSSION AND IMPLICATIONS

We have now highlighted the gaps to create a tangible, workable opportunities for future researchers in-line with recommendation of [10]. From the literature review, we have identified several antecedents. The review paints a picture of many studies covering Social or Behavioural related antecedents. A huge stream of information security related studies has focused majorly on individual related factors and less has covered the organizational related factors that drive information security policy compliance. Only one of the reviewed papers considered information security related factors. This means that there still exist some gaps that need to be filled with regards to technological and organizational factors that influence information security policy compliance by employees. With regards to insider threat mitigations from outsourced service organizations, the literature is very silent on how information security policy compliance can be addressed. Future studies therefore can direct attention to exploring how the information policy compliance can be achieved in organizations that we have no control over, and the only linkages exist being contractual agreements and service level agreements.

4.1 Theoretical Overview

We inductively identified several theoretical applications in the course of our review. Majority of articles analysed seem to have concentrated on the Social Behavioural related theories. This is in tandem with the fact that social/behavioural antecedents appear to be the majority standing at 57% in distributed extant works. Organizational related theories and Technological related theories however stand way below the social/behavioural related theories. We shall only give an over view of application of these theories and will not go deeper than descriptive narrative.

4.1.1 Reasoned Action Theory and Planned Behaviour Theory

False consistencies between component due to the awareness of the theory's assumptions by people has been one of the major criticism of Theory of Reasoned Action [13], however, the authors also noted the model's basic structure allowed for the ease of integration of the factors such as top organizational management and peers, a fact which they contended have been important in many previous research work that dealt with Information Systems success. Despite the criticism as indicated by [13], TRA has continued to find its space in scholarly work in Information System research when it comes to behavioural studies. Several constructs have been availed by different studies covering a wide range of areas of interests.

Several studies relating to the process of embracing technology have been conducted to determine factors that influence users to accept online systems or accept technology using TRA. These studies have employed or modified available constructs to suit their context. Theory of Reasoned Action (TRA) has arguably found its way across many Information Systems research realm especially those whose studies involve Organizational aspect and Human behavioural aspects of Information System research. The relationship between one's intention to comply and the corresponding actual compliance can be argued to have a direct correlation [14]. Several studies have also gone ahead to combine several theories in one study. For example, a study on information security policy for employees conducted empirically by Pahnila, Siponen, & Mahmood combined several theories in their studies namely *Protection* Motivation, *General Deterrence*, *Reasoned Action*, *Innovation Diffusion* and *Rewards* theories [14]. The constructs for Theory of Reasoned action in their study included Intention to comply and Actual compliance. In testing their hypothesis, the authors concluded that based on their results, the actual compliance received a statistically significant influence from intention to comply.

In Information systems research, Planned Behaviour (TPB) theory can be found in many recent scholarly works as well as much older studies. One of such studies is that of [15] in which the authors applied the TPB to study factors that contribute to compliance regime by employees with regards to information security policies whose findings revealed that one of the underlying basis of beliefs related to compliance was attitude [14]. Similarly, a study by Pahnila, Siponen, & Mahmood also noted that social constructs of Planned Behaviour theory with regards to awareness security facets referred to perceived influence together with perceived motivation associated with the respective perception of the norm surrounding an individual [14].

4.1.2 General Deterrence Theory

GDT has been applied in many studies dealing with by extension information security policy compliance [14]. GDT applies punishment as a tool for preventing crime and promotes required compliance by the whole society by creating conscious as well as unconscious inhibitions as preventive measures against crime. A study by Vaidyanathan and Berhanu, which looked into ways of converging user awareness and information security policies, applied GDT as a way of exploring how the security countermeasures impacted the flow within an organization, as well as the net effect it had on the organizational security performance [16].

4.1.3 Protection Motivation Theory

Employees' motivation through awareness initiative is suggested to have worked in many organizations where compliance was enhanced [17]. Equally works by Herath & Rao had earlier summarised in their work that three elements provided significant predictor of intentions to comply with policies and these were combination of; Severity of breaches threat perceptions together with response efficiency perceptions, self-efficiency perceptions, and costs related to response which had high possibility to impact on attitudes towards laid down policies; how organizations were committed and influence from social realms also significantly impacted on individual's intentions to comply; and last but not least availability of resource also was felt to have significantly influenced self-efficiency enhancement [18].

4.1.4 Technology – Organization – Environment Framework

Even though TOE has been widely applied in the study of Technology adoption, there are not many appearances of TOE framework in studies with information security policy compliance as a subject of study.

4.1.5 Institutional Theory

From an organizational related theory, only one article covered explicitly the Institutional Theory. Studies have shown that indicators of technological contexts and organizational contexts have an influence on how people in an organization comply with information security policies [19]. Within the Organizational context, coercive institutional pressures, normative institutional pressures, and mimetic institutional pressures have been found to contribute to information security policy compliance by [20].

4.2 Methodological Overview

Methodological overview also reveals quite substantive skewed applications of survey method. Survey approach accounted for more than 70% in the reviewed literature. This implies that majority of the reviewed articles were more of empirical studies.

4.3 Implications and Framework for Future Research

The implications of our review therefore can be summarised as a pointer to what areas still available for exploration such as the antecedents or predictors that influence information security policy compliance not only in terms of social or behavioural aspects, but a holistic approach covering both within the organization and without especially when the organizations that decides to outsource services and management of information assets envisage insider threat violations or weaker information security policy compliance in third party organizations.

4.4 Theoretical Framework for Future Research

As seen Fig3, our proposed framework introduces a dimension that factors in antecedents that relates to third party contracted entities as shown in the dotted box. By factoring in the antecedents that influences information security policy compliance among employees in third party organizations, researchers and practitioners alike will be addressing one of the missing links to a robust information security policy compliance regime.

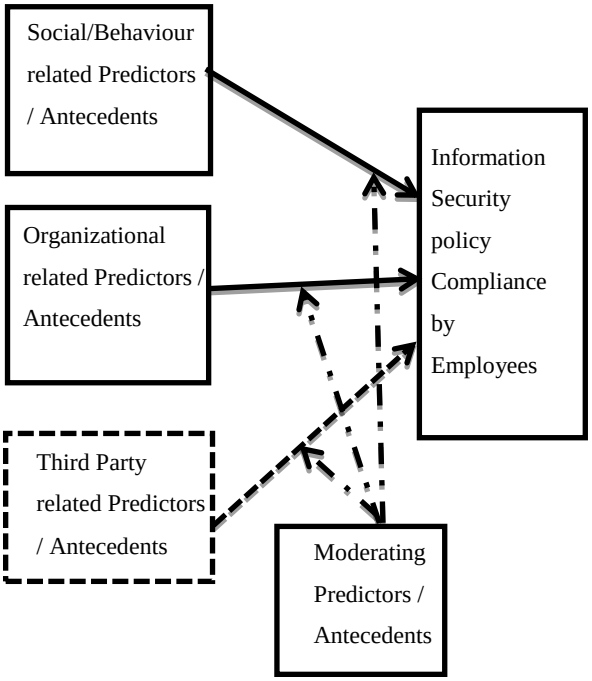

Fig 3: Information security policy compliance research framework - proposed

5. CONCLUSION

We had endeavored to understand the depth of antecedent coverage with regards to studies in information security policy compliance areas of inquiry. We have elaborated in depth the antecedents as they appear in extant literature within a systematic time range of between 2004 and 2018. We have identified several unexplored areas by expounding the scope of insider threats and insiders to include insiders in organizations contracted to handle information assets and services on behalf of organizations. In reaching this objectives, we applied concept-centric approach as suggested by [10] to come up with categories of thematic areas to focus our review on namely: (1) Organizational related antecedents, (2) Social/behavioural related antecedent, (3) Technological related antecedents and based on our expanded focus of insiders, we proposed (4) Third Party contracted entities. We then proposed a framework to guide future researchers based on our thematic outcomes as a way of addressing the gaps that emerged based on the broadened insider definition.We would like to highlight four major areas of contribution; Knowledge Contribution, Theoretical contribution, Methodological contribution, and Contribution for practitioners in the field of Information security policy management. Our expanded definition and discourse regarding insider threats and insiders will be helpful to build the already existing body of knowledge and drive future researchers to come up with more robust and replicable taxonomies of insiders. It is our submission that for a proper insider threats management to be in place, understanding who we are dealing with is paramount. We have also proposed a theoretical framework that can be considered by researchers to develop knowledge on the area of information security policy compliance in a holistic manner as seen in Fig 3. The main contribution of this paper from the new proposed framework is the added dimension of Third-Party related Predictors / Antecedents as shown in the dotted box in Fig 3.By exploring and giving a descriptive narrative of the extent of appearances of a few Theories in the reviewed papers, this review provides a pointer to the direction in which future researchers can explore. For example, very few

reviewed papers looked at organizational related theories yet as already seen in some reviewed articles, organizations play a very important role to influence each other to strengthen the information security policy compliance regime or influence employees' behaviour in relation to compliance.

The descriptive results show how reviewed papers have not concentrated on other methodological approaches such mixed method. It is our submission that the by embracing other methodologies in conjunction with positivist methodologies would bring more impetus and strengthen the empirical outcomes of information security policy compliance studies.Contributions towards the practitioners in the field of information security management can be found in the fact that the review will better inform the plans on how to engage third parties with regards to how they enforce information security policy compliance regimes in their jurisdictions. Appreciating the fact that we have phantom insiders in the third party contracted organizations such as cloud providers will bring to attention the need to broaden the scope of addressing compliance by practitioners.

We recommend future researchers to diversify their studies predicated on the expanded insider threats definition and classifications. Finally, the proposed framework provides a rich area to be taken up in empirical based studies with further recommendation that more of mixed methods be considered.

6. REFERENCES

[1] R. F. Trzeciak, "SEI Cyber Minute: Insider Threats," 2017.

[2] PwC, "Global Economic Crime Survey 2016: US Results," 2017.

[3] M. L. Collins, M. C. Theis, R. F. Trzeciak, J. R. Strozer, J. W. Clark, D. L. Costa, T. Cassidy, M. J. Albrethsen and A. P. Moore, "Common sense guide to prevention and detection of insider threats 5th edition," CERT, Software Engineering Institute, Carnegie Mellon University, 2016.

[4] McAfee, "Cloud Adoptionand Risk Report," 2019.

[5] B. Lebek, J. Uffen, M. Neumann, B. Hohler and M. H. Breitner, "Informationsecurity awareness and behavior: a theory-based literature review," Management Research Review, vol. 37, no. 12, pp. 1049-1092, 2014.

[6] P. Balozian and D. Leidner, "Review of IS Security Policy Compliance: Toward the Building Blocks of an IS Security Theory," the DATABASE for Advances in Information Systems, vol. 48, no. 3, pp. 11-43, 2017.

[7] W. A. Cram, J. G. Proudfoot and J. D'Arcy, "Organizational information security policies: a review and research framework," European Journal of InformationSystems, vol. 26, no. 6, pp. 605-641, 2017.

[8] M. J. Alhanahnah, A. Jhumka and S. Alouneh, "A Multidimension Taxonomy of Insider Threats in Cloud Computing," The Computer Journal, vol. 59, no. 11, p. 1612–1622, 2016.

[9] T. Webster and R. T. Watson, "Analyzing the Past to Prepare for the Future: Writing a Literature Review," MIS Quarterly, vol. 26, no. 2, pp. xiii-xxii, 2002.

[10] F. Rowe, "What literature review is not: diversity, boundaries and recommendations," European Journal of Information, vol. 23, no. 3, p. 241–255, 2014.

[11] G. Pare, M. Trudel, M. Jaana and S. Kitsiou, "Synthesizing Information Systems Knowledge: A Typology of Literature Reviews," Information & Management, vol. 52, no. 2, pp. 183-199, 2015.

[12] A. Harzing, "Journal Quality List," 29 July 2018. [Online]. Available: https://harzing.com/resources/journal-quality-list. [Accessed January 2019].

[13] P. P. Mykytyn, JR. and D. A. Harrison, "The Application of the Theory of Reasoned Action to Senior Management and Strategic Information Systems," Information Resources Management Journal, vol. 6, no. 2, pp. 15-26, 1993.

[14] S. Pahnila, M. Siponen and A. Mahmood, "Employees' Behavior towards IS Secur ity Policy Compliance," in Proceedings of the 40th Hawaii International Conference on System Sciences - 2007, 2007.

[15] B. Bulgurcu, H. Cavusoglu and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," MIS Quarterly, vol. 34, no. 3, pp. 523-548, 2010.

[16] G. Vaidyanathan and N. Berhanu, "Impact of Security Countermeasures in Organizational Information Convergence: A Theoretical Model," Issues in Information Systems, vol. 13, no. 2, pp. 21-25, 2012.

[17] A. D. Veiga, "The Influence of Information Security Policies on Information Security Culture: Illustrated through a Case Study," Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015), p. 22, 2015.

[18] T. Herath and R. H. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations," European Journal of Information Systems, vol. 18, no. 2, pp. 106-125, 2009.

[19] A. AlKalbani, H. Deng and B. Kam, "Investigating the Role of Socio-organizational Factors in the Information Security Compliance in Organizations," in Australasian Conference on Information Systems, Australia, Adelaide, 2015.

[20] A. AlKalbani, H. Deng, B. Kam and X. Zhang, "Investigating the Impact of Institutional Pressures on Information Security Compliance in Organizations," in Australasian Conference on Information Systems, Australia, Wollongong, 2016.