# 38. Information Systems Security Policy Violation: Systematic Literature Review on Behavior Threats by Internal Agents

Kennedy Njenga
University of Johannesburg
knjenga@uj.ac.za

## *Abstract*

Systematic literature review (SLR) addresses the question of structured literature searches when dealing with a potentially large number of literature sources. An example of a large number of literature sources where SLR would be beneficial can be found in the Information systems security literature which touches on internal agents' behavior and tendencies to violate security policies. Upon close examination, very few studies have used SLR in the work. This work presents an insightful approach to how SLR may be applicable in the domain of Information Systems security. The article presents a summary of the SLR approach contextualized in the domain of IS security in order to address such a gap. Rigor and relevance is systematized in the work through a pre-selection and coding of literature using *Atlas.ti*. The outcome of the SLR process outlined in this work is a presentation of literature in three pre-determined schemes namely, the theories that have been used in information systems security violations literature, categorization of security violations as presented in literature; and the contexts that these violations occur. The work concludes by presenting suggestions for future research.

## *Keywords*

Systematic Literature Review (SLR), Information Security, Security Policies, Violations. Behavior.

## 1. Introduction

Systematic literature review (SLR) addresses the question of structured literature searches when dealing with a potentially large number of literature sources. An example of literature sources where SLR would be beneficial can be found in the Information Systems (IS) security literature and especially literature that touches on internal agents as threats to systems and their predisposition to violate security policies. Most scholarly work approach systems security violations from various perspectives using popular IS theories such as Deterrence theory, (Straub and Nance, 1990) Neutralization, (Siponen and Vance, 2010) Protection Motivation, (Warkentin, Malimage and Malimage, 2012; Siponen, Mahmood and Pahnila, 2014; Browne, Lang and Golden, 2015) to name but a few.

Upon close examination, very few of these studies have used SLR in the domain of IS security. A review of such studies suggests an inadequacy of a replicable step-by-step structure around the evidence collected and validated in the literature review process. Indeed Okoli and Schabram,

(2010) have affirmed that "*information systems scholars tend to be unaware of the need for structure in literature reviews*". The importance of having structure around literature reviews as stated by Morrell, (2008) has been "*to advance policy and practice by providing the best evidence available from research".* Importantly, the distinctiveness of structure in literature reviews is best demonstrated by SLR which is a prescription on the literature review process (Boell and Cecez-Kecmanovic, 2015).

The purpose of this article is to therefore adopt the SLR protocol to address literature review extensiveness to date in IS security. The context being information security policy violation by internal agents arising as result of their specific behaviors. The SLR protocol is *systematized* methodically in this work to delineate security linked behavior that leads to policy violation in a *non-biased*, *replicable*, *scientific* and *rigorous* manner (Morrell, 2008; Boell and Cecez-Kecmanovic, 2015). The article is timely since despite the increasing adoption of SLRs in other domains, SLR has largely gone unnoticed in the IS security literature (Boell and Cecez-Kecmanovic, 2015). Documenting SLR within the domain of IS security addresses such a gap.

In addressing the context of SLR within the domain of IS security, the article is presented as follows: introduction of main theme and context; discussion of important aspects of SLR with focus on the internal agent as a threat to information systems and security policy violation; and, representation of literature with emphasis on the coding procedure recommended by SLR protocol. The penultimate section is a write-up of findings regarding the literature review outcome and the conclusions thereon.

## 2. Aspects of Systematic Literature Review

'*Literature review'* can be regarded as a process by which a scholar will identify, analyze, assess and synthesize earlier research (Boell and Cecez-Kecmanovic, 2014). Literature reviews in general can be presented as parts of research reports (e.g. in papers or theses) or stand-alone literature publications. Literature reviews often examine and critically assess existing knowledge in a particular problem domain and will form the foundation for identifying weakness and poorly understood phenomena (Khoo, Na and Jaidka, 2011). Many approaches have been suggested for conducting an effective literature review; Bandra, Miskon and Fielt, (2011) suggests using thematic analysis and qualitative research for analyzing a body of literature. Grounded theory as a means of conducting literature reviews has equally been suggested by Wolfswinkel, Futmueller and Wilderom (2013). Scholars such as Boell and Cecez-Kecmanovic (2014) have also provided a framework of literature review using Hermeneutics.

The Systematic Literature Review (SLR) approach (protocol) demonstrated in IS studies, (Atkins and Louw 2000; Amrollahi *et al.,* 2013) addresses the role and importance of literature search process in a dissimilar manner to the above mentioned papers which makes it an interesting structured approach. Boell and Cecez-Kecmanovic, (2015) provide a detailed account of the origins and procedures of SLR which is seen as a unique prescriptive approach that addresses the identification, selection, assessment and synthesizing of evidence from the literature. SLR continues to make profound inroads into the IS literature (Boell and Cecez-Kecmanovic, 2015). SLR avoids bias in the review process because of the rigor associated with the method (Oxman, 1995). Rigor is achieved by way of developing a literature review protocol that specifies criteria

for selecting and assessing articles. The following section explains how rigor is systematized in SRL on the issue of information security policy violation by internal agents.

## 2.1 Systematizing rigor in Systematic Literature Review

To contextualize the phenomenon of information security policy violation by internal agents, rigor has been systematized by adopting SLR in four phases as suggested by Bandara *et al.*, (2011). This is shown by **Figure 1** below.

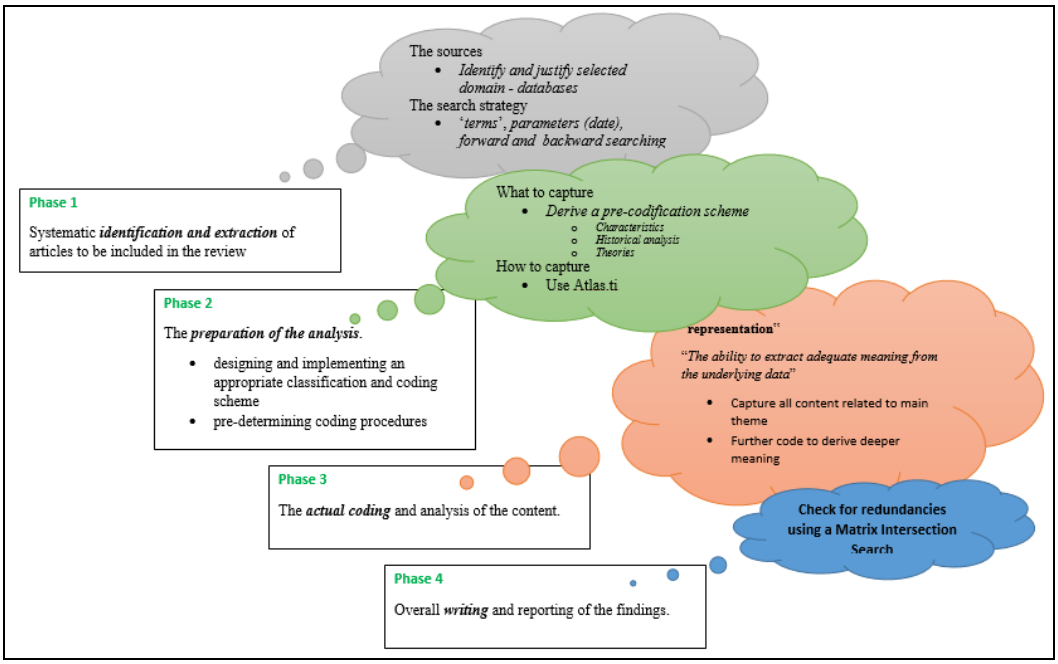


**Figure 1**: Systematic Literature Review of Information Security Policy Violation in Phases
Adopted from: (Bandara, Miskon and Fielt, 2011)

The first phase involved systematically identifying and extracting articles related to the violation of security policies by internal agents through making effort to identify as many publications as possible that remained relevant within the domain of IS security for this purpose. This work is presented in ***Section 2*** of this article. The second phase involved designing a way to systematically capture literature using a predetermined coding scheme. This work is presented in ***Section 3*** of this article. The third phase involved representation of the main theme (policy violation by internal agents) through qualitatively coding literature sources. Coding involved directly capturing content related to the main theme and further coding to derive deeper meaning. The use of the qualitative analysis software *Atlas.ti* was used for this purpose. This work is presented in ***Section 4*** of this article. The final phase involved writing up the findings of the literature review process and suggested action for future research. This work is presented in ***Section 5*** of this article.

## 2.1 Systematizing literature source

SLR by definition will differ from a traditional literature review in that the scope is highly specific (Boell and Cecez-Kecmanovic, 2015). In context to the case, the need to understand

information security policy violation by internal agents is specified by using the framework outlined by **Figure 1** in a standardized and systematized process. In terms of selecting the right sources, the domain of interest was Information Systems (IS) security with constructs of '*behavior*' and '*violation*' borrowed from the domains of Psychology (Chapman and Brothers, 2006). Pre-selection of articles in IS specific databases that included constructs of '*internal agents'* '*security threats'* and '*security policy violations'* was done in such a way that the process would be *replicable* and *objective* (Okoli and Schabram, 2009). **Table 1** below provides data regarding the resources used, the justification for the selection of literature sources and number of items used.

| ***Source*** | ***IS Specific*** | ***Articles extracted*** | ***Articles included (excludes duplicates in other databases)*** |
|---|---|---|---|
| 1. | ACM Digital Library | 62 | 8 |
| | Emerald Management Extra | *25* | *3* |
| | IEEE Xplore | *2* | *2* |
| | ScienceDirect | *24* | *6* |
| | ProQuest | *20* | *2* |
| 2. Google Scholar | | *14* | *4* |
| 3. AIS eLibray ** search term '*violations*' '*policy non-compliance'* | | *28* | *19* |
| 4. ***Senior Scholars' Basket of Journals (8) | | - | - |
| **Total** | | ***175*** | ***44*** |

*** advanced search terms: security+ policy+ violations in title : peer reviewed articles only*
**** items found in previous databases*

**Table 1**: Literature Sources

## 2.2 Systematizing search strategy

What was imperative in terms of systematizing the search strategy, was to firstly identify important terms in the title, abstract and key words of relevant articles that focused on internal threat agents, and violation of security policies. To achieve rigor in this process, it was necessary to specify the criteria for inclusion and exclusion of published work. Of the 175 articles that were searched using the parameters; '*security*' + '*policy'* + '*violation*', screening was done and technical papers that did not deal with behavior were excluded (Atkins and Louw, 2000; Okoli and Schabram, 2010). In addition the search term '*non-compliance'* was also used to denote violation. The use of this alternative terminology was important because of the need to address a well-known problem in information retrieval described as the '*indeterminacy of language'* Blair (2006). The criteria carried out to screen additional but relevant papers in the body of knowledge identified in **Table 1** above is shown by **Table 2** below. A backward and forward search were also conducted (Levy and Ellis 2006).

# 3. Systematic Capturing of Literature

Bandara *et. al.,* (2011), recommend important aspects in systematically analyzing literature that has been considered from the identified literature sources and systematized searches. What is essentially recommended, is to firstly determine what to capture and secondly, how to capture

the literature by way of establishing a '*pre-coding scheme'*. An analysis of past meta-literature review papers (Orlikowski and Baroudi 1991, Vessey et al. 2002) presented by Bandara *et. al.*, (2011), proposes various themes that have been used in IS literature. Three of these themes have been applied for meta-review namely; *theories, characteristics* and *contexts* presented in literature.

| ***Search terms*** | ****Search in title & abstract*** | ***Backward search*** | ***Forward search*** | ***Total*** |
|---|---|---|---|---|
| ***Number of articles extracted** | - | - | - | 175 |
| **Number of articles selected for inclusion** | 40 | 3 | 4 | 44 |
| ****Number of articles excluded** | - | - | - | 131 |

**number of articles extracted – see **Table 1***

***Justification for exclusion of articles: Articles screen for methodical soundness found lacking*

**** advanced search in title (security + policy + violation) and (non-compliance)*

**Table 2**: Search strategy

## 3.1 Designing a predetermined coding scheme

Following the SLR protocol we derived a pre-coding scheme that addressed the most pertinent goals of the study namely;

- **Theories** used in information systems security violations
- **Characteristics** of various types of information security violations;
- **Contexts** of studies in Security violations;

## 3.2 Determining coding procedure

*Atlas.ti* was used for the first-level analysis. This tool enabled the capturing of content relating to the three themes by assigning nodes for analyzing each theme. Regarding themes outlines earlier, ideas pre-determined included; '*factors influencing violation'*, '*deterrence of violation*', and '*categories of threat agents*' and were coded. Only fragments of sentences were coded.

# 4. Representation: Coding Internal Agent Behavior and Security Policy Violation

## 4.1 Coding

The coding process identified important relationship between theory used in literature and contexts scholar examined security violations within this domain. The coding process therefore provided for a meta-view of the various publications that underlined such relationship. No

particular structure was used in mapping and classifying codes, although the mapping and structuring was pre-guided by the three themes identified earlier. All selected 44 articles (in PDF format) were uploading into *Atlas.ti*. Articles were indexed using author surnames and year of publication. Generic codes were assigned in contexts to empirical work presented in the articles. In adhering to the initial pre-coding scheme, each article was reviewed and coded. **Figure 2** below illustrates an example of the coding procedure used to assigned indexed articles to the theories the articles were based on. Coding was done, moving from left to right in a historical chronology of articles with the exception of articles that did not use any theoretical lens. **Table 3** that follows presents an example of a systematic summary of the coding of articles that was carried out.

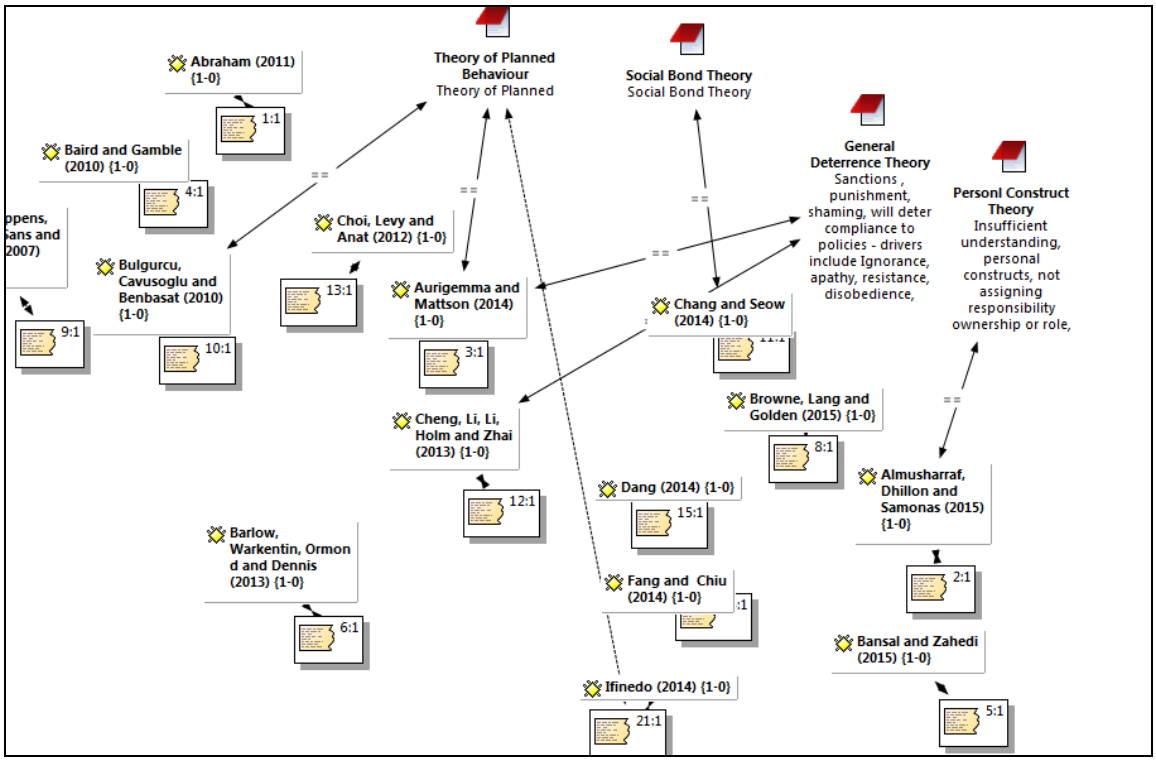


**Figure 2**: *Atlas.ti* indexing, coding for author and theory

| *Theories used* | *Systematized Literature Review Sources* | *Influences to Violating Security Policies - codes* |
|---|---|---|
| *Personal Construct Theory,* | [2]Almusharraf, Dhillon and Samonas (2015); | *Insufficient understanding, personal constructs, not assigning responsibility ownership or role,* |
| *Theory of Planned Behavior* | [2]Aurigemma and Mattson (2014); [2]Bulgurcu, Cavusoglu and Benbasat (2010); [2]Ifinedo (2014) ; [3]Takemura (2014); [2]Wei and Hsu (2014) ; [3]Herath and Rao (2009) | *sanctions are significant antecedent to user intentions to comply with security policies* |
| *General Deterrence Theory* | [2]Aurigemma and Mattson (2014); [3]Cheng, Li, Li, Holm and Zhai (2013); [3]Hovav and D'Arcy (2012) ; [3]Siponen and Vance (2010); [3]Takemura (2014) ; [3]Ugrin and Pearson (2010); [3]Warkentin, Malimage and Malimage (2012) ; [3]Herath and Rao (2009); [2]Straub 1990; | Sanctions , punishment, shaming, will deter compliance to policies – drivers include *Ignorance, apathy, resistance, disobedience,* |
| *Attribution theory* | [3]Bansal and Zahedi (2015) ; | *emotional displeasures, perceived justices of organization,* |
| *Organizational justice theory* | [3]Bansal and Zahedi (2015); [3]Dang (2014); | *commercial incentive/profit,* |
| *Theory of neutralization* | [3]Barlow, Warkentin, Ormond and Dennis (2013); [3]Siponen and Vance (2010) | *Neutralization to justify deviant action, rationalization ; Deference of necessity, denial of injury, Metaphor of ledger* |
| *Framing theory* | [3]Barlow, Warkentin, Ormond and Dennis (2013); | *Individual propensity and moral belief, perceived justice of punishment, cognitive processing, moral reasoning, mandatoriness of policies* |
| *Protection Motivation Theory* | [3]Browne, Lang and Golden (2015); [3]Siponen, Mahmood and Pahnila (2014); [3]Warkentin, Malimage and Malimage (2012); [3]Warkentin, McBride, Carter and Johnston (2012) ; [3]Herath and Rao (2009); | *Hedonistic feelings (thrill, pleasure), Intrinsic benefit*<br>*Emotional state: Sanctions can moderate* |
| *Rational Choice Theory* | [3]Browne, Lang and Golden (2015) ; [3]Bulgurcu, Cavusoglu and Benbasat (2010); [3]Vance and Siponen (2012) ; [3]Wei and Hsu (2014) | *rationality-based ; threat appraisal and coping appraisal* |
| *Sensemaking theory* | [2]Chang and Seow (2014) | *perceived clashes between the underlying values* |
| *Social bond theory.* | [3]Cheng, Li, Li, Holm and Zhai (2013); [3]Safa, Von Solm and Furnell (2016) | *Weaker social bonds more likely to engage in a white-collar crime; attachment, commitment, involvement* |
| *General Strain Theory* | [3]Dang (2014); | *pre-kinetic events: disgruntlement ,Job dissatisfaction, sanction pressure* |
| *Decomposed Theory of Planned Behavior* | [2]Molok, Ahmad and Chang (2010); [3]Herath and Rao (2009) | attitude, subjective norm and perceived behavioral control explain violations |
| *Social Bond Theory* | [3]Ifinedo (2014); [3]Safa, Von Solm and Furnell (2016); [3]Cheng, Li, Li, Holm and Zhai (2013) | Lacking in knowledge sharing, collaboration, intervention and experience leads to violations |
| *Involvement theory* | [3]Safa, Von Solm and Furnell (2016) ; | Attachment, commitment, involvement and belief |
| *Organisational commitment* | [3]Herath and Rao (2009) | *penalties, social pressure and intrinsic motivation, can explain variance in employees' intention to comply with rules* |
| *Cognitive Evaluation Theory (CET)* | [3]Siponen, Mahmood and Pahnila (2014); | *Cognitively evaluate: ( threat and coping appraisals)* |
| *Theory of Reasoned Action (TRA)* | [3]Siponen, Mahmood and Pahnila (2014); | Attitudes and subjective norms |
| *General theory of crime* | [2]Hu, West and Smarandescu (2014) ; | low self-control: propensity toward criminal behavior/ violations |
| ***1**No theory Used in articles (literature)*** | Choi, Levy and Anat (2012), D'Arcy, Gupta, Tarafdar and Ofir Turel (2014); D'Arcy et al. 2009; Guo and Yuan (2012); Guo et al. 2011; Hu *et. al*, (2011); Hu, West and Smarandescu (2014); Johnston and Warkentin (2010) ; Kraemer and Carayon (2007) ; Kretzer and Mädche (2015); Maasberg (2014); Martin and Imboden (2014) ; Siponen and Vance (2014); Vance et al., 2012) ; Willison and Warkentin (2013); *Crossler et al. (2013)* | |

[1**] *conceptual papers*

[2] *Theory used with empirical evidence in article –empirical research papers*

[3] *Article uses more than one theoretical lens – Some articles applied multi-theories in the empirical work*

**Table 3**: Summary of Systematic Literature review for Security Policy Violations

# 5. Findings: Information Security Policy Violation

## 5.1 Information Security Policy Theories used in Literature

From the SLR carried out, it was clear that many researchers have addressed research in information security violation from various theoretical underpinnings and by providing empirical evidence supporting such research. Some articles used one theory although many applied multiple theories. From a theory-in-use perspective, interesting and novel theories used in IS security literature were coded. General Deterrence Theory, was coded to be the most popular theory with six articles applying this theory in scholarly work (see **Table 2**). Protection Motivation Theory also remained popular with five articles applying this theory in the studies. An interesting approach to violation of security polities was revealed by the works of Brunel, Cuppens, Cuppens, Sans and Bodeveix (2007) who consider breach of permission and obligation requirements from a behavior model that uses 'Labeled Kripke Structures'. In more recent studies Hu, West and Smarandescu (2014) look at security violations from a Lab based neuroscience perspective and consider event-related brain potentials (ERPs) using the general theory of crime. What is novel is how they apply brain imaging technologies-magnetic resonance imaging (fMRI) and electroencephalography (EEG) to explain self-control as an inhibitor of desire for immediate gratification and how low self-control could short circuit moral judgement and rational choice. There were instances where scholarly work was coded for two or more theories used by scholars to explain information security policy violations (Aurigemma and Mattson, 2014; Bansal and Zahedi, 2015; Barlow, Warkentin, Ormond and Dennis, 2013; Browne, Lang and Golden, 2015; Cheng, Li, Li, Holm and Zhai, 2013).

## 5.2 Information Security Policy Violation categories and characteristics

An important finding coming from the systematic literature review is the various categorization of threats behaviors by internal agents. Coded work and memos drawn from the SLR approach show that different scholars categorize security violations differently. There was disharmony in the categorization process. Aurigemma and Mattson (2014) categorize behavior as either; (1) malicious (intentional and deviant) or (2) non-malicious (volition and non-volition). Barlow, Warkentin, Ormond and Dennis (2013) postulate three categories as; (1) malicious, (2) non-malicious and (3) deviant behavior. Dang (2014) also suggests three alternative categories as (1) non-volitional noncompliance, (2) volitional (but not malicious) noncompliance and (3) intentional malicious abuse. Guo and Yuan (2012) outlines four categories which include; (1) knowingly break rules (employees violate security policies that they know exist); (2) are voluntary (actions are not forced by other parties, e.g. supervisors); (3) are intentional (employees make conscious decisions to engage in the action); and (4) non-malicious (employees are not trying to cause damage). Kraemer and Carayon (2007) considers two categories that include, violations of malicious intent (e.g., insider threats, hackers, terrorists) and (2) violations of a non-malicious nature. Martin and Imboden (2014) also outlines three categories that include; (1) passive, non-volitional, (2) volitional, non-malicious, and (3) intentional, malicious. Siponen and Vance (2014) talk of non-deliberate or deliberate violations.

## 5.3 Information Security Policy Violation contexts

The contexts for security policy violations was coded and shown to vary from one scholarly work to another. Cheng, Li, Li, Holm and Zhai (2013) for instance looks at how an internal agent's weaker social bonds to their mangers, co-workers, and organizations would most likely

influence their willingness to engage in violations. D'Arcy, Gupta, Tarafdar and Ofir (2014) work on the "dark side" of IT use; suggest that the motivators to violation would be variables such as IT-usage-related stress, work overload, interruptions, addiction, and beliefs (security-related). These are moderated by sanctions and moral considerations. Kraemer and Carayon (2007) outlines violations through human error, while Maasberg (2014) outlines the taxonomy of insider espionage as personal crisis, disposition for civil disobedience which could lead to intellectual property theft, fraud or sabotage. Siponen and Vance (2010) present neutralization techniques that are used by internal agents to decrease the perceived harm of their policy violations. Ugrin and Pearson (2010) have conducted empirical studies on cyber-loafing and the viewing and exposing others to sexual and pornography as a form of noncompliance to policies. Warkentin, Malimage and Malimage (2012) suggest that depending on the types of sanctions present positive (reward) or negative (punishment), these may influence employees differently across different cultures. Interestingly, Takemura's (2014) empirically studies in Japanese culture suggests that violating security policy cannot necessarily be deterred through the threat of punishment.

### 5.4 Suggestions for Future Research

With the exception of Guo *et. al.,* (2011), who has theories on non-malicious security violations most other studies have been based on surveys that have not differentiated nor effectively categorized between for instance passive volitional behavior and non-passive malicious (see section 5.2 above). A study that effectively proposes a framework of these categorizes would be of great value to industry and practice.

## 5. Conclusions

This article has taken an objective perspective and undertaking for incorporating the Systematic Literature Review (SLR) approach into the domain of IS security. SLR was contextual to information security policy violations by internal agents. The SLR outcomes identifies various theories that have been used in literature to explain violations, the categorization of various violations and the contexts that these violations occur. The article expands the body of knowledge by using SLR in this regard. The need to understand what literature says around IS security policy violations is not only important but timely. This is true considering that the study of IS security violations continue to receive a great deal of attention in IS literature. The article addresses the SLR gap by opening up a discussion on why different scholars categorize security violations differently. What is proposed therefore is work that harmonizes this categorization across different scholarly work in an objective, scientific and replicable way. This can be a good basis to justify future research. This work reveals depth in the body of knowledge around the study of IS security violations. A much broader study embarking on more qualitative and systematic studies that touch on how these violations can be managed and addressed is encouraged. Such a study would further the understanding of violations in information systems security.

## References

Almusharraf, A. Dhillon, G. and Samonas S. (2015) "Mismatched Understanding of IS Security Policy: A RepGrid Analysis", *Proceedings of the 21st Americas Conference on Information Systems (AMCIS),* Puerto Rico, pp. 1-12.

Amrollahi, A., Ghapanchi, A.H. and Talaei-Khoei, A. (2013). "A Systematic Literature Review on Strategic Information Systems Planning: Insights from the past decade", *Pacific Asia Journal of the Association for Information Systems* 5(2), pp. 39–66.

Atkins, C. and Louw, G. (2000). Reclaiming Knowledge: A Case for Evidence Based Information Systems Reclaiming Knowledge: A Case for Evidence-Based Information Systems, in *Proceedings of the European Conference on Information Systems* (*ECIS*), Vienna, Austria, Paper 28.

Aurigemma, S. and Mattson, T. (2014) "Do it OR ELSE! Exploring the Effectiveness of Deterrence on Employee Compliance with Information Security Policies", *Proceedings of the 20th Americas Conference on Information Systems (AMCIS)* Savannah, Georgia, USA, pp. 1-12.

Bandara, W., Miskon, S. & Fielt, E. (2011). "A systematic, tool-supported method for conducting literature reviews in information systems". *Proceedings of the 19th European Conference on Information Systems (ECIS)*, pp. 1-13.

Bansal, G. and Zahedi, F.M. (2015), "Trust violation and repair: The information privacy perspective" *Decision Support Systems* 71, pp. 62–77.

Barlow, J.B., Warkentin, M., Ormond D. and Dennis, A.R. (2013), "Don't make excuses! Discouraging neutralization to reduce IT policy violation" *Computers & Security* 39, pp.145-159.

Blair, D. (2006). "*Wittgenstein, Language and Information. Back to the Rough Ground!"* Dordrecht, Springer.

Boell, S. K., and Cecez-Kecmanovic, D. (2015). "On being 'systematic' in literature reviews in IS". *Journal of Information Technology, 30* (2), pp. 161-173.

Boell, S. K., and Cecez-Kecmanovic, D. (2014). "A Hermeneutic Approach for Conducting Literature Reviews and Literature Searches". *Communications of the Association for Information Systems, 34* (12), pp. 257-286.

Browne, S. Lang M. and Golden W. (2015), "The Insider Threat - Understanding The Aberrant Thinking Of The Rogue"Trusted Agent" ",*Proceedings of the 23rd European Conference on Information Systems* (*ECIS*), pp. 1-11.

Brunel, J. Cuppens, F., Cuppens, N., Sans, T, and Bodeveix, J.P. (2007) "Security Policy Compliance with Violation Management" *Proceedings of the ACM workshop on Formal methods in security engineering,* pp. 31-40

Bulgurcu, B. Cavusoglu, H. and Benbasat, I. (2010), "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness", *MIS Quarterly* 34 (3) pp. 523-548.

Chapman, B. and Brothers, P. (2006). "Database Coverage for Research in Management Information Systems". *College & Research Libraries*, pp. 50 – 62.

Chang and Seow (2014), "Effects of IT-Culture Conflict and User Dissatisfaction on Information Security Policy Non-Compliance: A Sensemaking Perspective", *Proceedings of the* 20th Americas Conference on Information Systems (*AMCIS*), Savannah, Georgia, USA, pp. 1-12.

Cheng, Li, Li, Holm and Zhai (2013), "Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory", *Computers & Security* 39 pp. 447-459.

Choi, M., Levy Y. and Anat, H. (2012), "The Role of User Computer Self-Efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills Influence on

Computer Misuse", *pre-ICIS workshop on Information Security and Privacy (SIGSEC). Paper 29.*

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013), "Future directions for behavioral information security research", *Computers & Security* 32 pp. 90-101.

D'Arcy, J., Gupta, A., Tarafdar, M. and Ofir T. (2014), "Reflecting on the "Dark Side" of Information Technology Use", *Communications of the Association for Information Systems,* 35(5), pp. 109-118.

D'Arcy, J., Hovav A, and Galletta D. (2009) "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach" *Information Systems Research* 20(1), pp. 79-98.

Dang, D.P.T. (2014), "Predicting Insider's Malicious Security Behaviours: A General Strain Theory-Based Conceptual Model", *Proceedings of the International Conference on Information Resources Management (CONF-IRM)*

Guo and Yuan (2012), "The effects of multilevel sanctions on information security violations: A mediating model" *Information & Management*, 49 pp. 320–326.

Guo, K.H., Yuan Y., Archer N.P.and Connelly C.E. (2011) "Understanding non-malicious security violations in the workplace: a composite behavior model". *Journal of Management Information Systems* 28(2), pp. 203-36.

Herath, T. and Rao H. R. (2009), "Protection motivation and deterrence: a framework for security policy compliance in organisations", *European Journal of Information Systems,* 18 pp. 106–125.

Hovav, A. and D'Arcy, J. (2012) "Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the US and South Korea". *Information Management* 49(2), pp. 99-110.

Hu, Q., Xu, Z., Dinev, T., and Ling, H. (2011) "Does deterrence work in reducing information security policy abuse by employees?" *Communications of the ACM*, 54(6), pp. 54-60.

Hu, West and Smarandescu (2014), "The Role of Self-Control in Information Security Violations: Insights from a Cognitive Neuroscience Perspective", *Journal of Management Information Systems* 31 (4), pp. 6–48.

Ifinedo, P. (2014), "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition" *Information & Management* 51 (1) pp. 69-79.

Johnston, A.C. and Warkentin M. (2010) "Fear appeals and information security behaviors: an empirical study". *MIS Quarterly* 34(3), pp.549-566.

Kraemer S. and Carayon P. (2007), "Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists" *Applied Ergonomics* 38 pp.143–154.

Kretzer, M. and Mädche A. (2015), "Which are the Most Effective Measures for Improving Employees' Security Compliance?" *Proceedings of the 36th International Conference on Information Systems* (ICIS), Fort Worth. pp. 1-17.

Khoo, C. S. G., Na, J.-C., and Jaidka, K. (2011), "Analysis of the Macro-level Discourse Structure of Literature Reviews", *Online Information Review*, 35(2), pp. 255–271.

Levy, Y., and Ellis, T.J. (2006). "A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research". *Informing Science Journal* (9), pp.181-212.

Maasberg (2014), "Insider Espionage: Recognizing Ritualistic Behavior by Abstracting Technical Indicators from Past Cases" *Proceedings of the 20th Americas Conference on Information Systems (AMCIS)* Savannah, Georgia, USA, pp. 1-10.

Martin, N.L. and Imboden T.R. (2014), "Information Security and Insider Threats in Small Medical Practices" *Proceedings of the 20th Americas Conference on Information Systems (AMCIS)* Savannah, Georgia, USA, pp. 1-9.

Molok, A., Ahmad, A. and Chang S. (2010), "Understanding the Factors of Information Leakage through Online Social Networking to Safeguard Organizational Information" *Proceedings of the 21st Australasian Conference on Information Systems* (*ACIS*), paper 62, Brisbane.

Morrell, K. (2008). "The Narrative of 'Evidence Based' Management: A polemic", *Journal of Management Studies* 45(3), pp. 613–635.

Okoli, C. and Schabram, K. (2009). "Protocol for a Systematic Literature Review of Research on the Wikipedia", *Working Papers on Information Systems,* Sprouts: 9 (65).

Okoli, C. and Schabram, K. (2010). "A Guide to Conducting a Systematic Literature Review of Information Systems Research", *Working Papers on Information Systems,* Sprouts: 10 (26).

Orlikowski, W.J. and Baroudi, J.J. (1991) Studying Information Technology in Organizations: Research Approaches and Assumptions, *Information Systems Research*, 2(1), pp. 1-8.

Oxman, A.D. (1995). "Checklists for Review Articles", in I. Chalmers and D.G. Altman (eds.) *Systematic Reviews,* London: BMJ, pp. 75–85.

Safa, N.S., Von Solm R. and Furnell S. (2016), "Information security policy compliance model in organizations", *Computers & Security* 56 pp. 70-82.

Siponen M. and Vance, A. (2010), "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations" *MIS Quarterly* 34(3), pp.487-502.

Siponen and Vance (2014), "Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations", *European Journal of Information Systems,* 23, pp. 289–305.

Siponen, Mahmood and Pahnila (2014), "Employees' adherence to information security policies: An exploratory field study", *Information & Management* 51 pp. 217–224.

Straub, D.W. (1990) "Effective IS Security: An Empirical Study", Information Systems Research, (1)3, pp. 255–276.

Takemura, T. (2014), "Empirical Analysis of Intentional Security Policy Violation in the Workplace" *Saga University economic review* 46(6) pp. 21-40.

Ugrin, J.C. and Pearson, J.M. (2010), "Understanding The Effect Of Deterrence Mechanisms On Cyberloafing: Exploring A General Deterrence Model With A Social Perspective" *Proceedings of the 31ST International Conference on Information Systems,* (ICSI) St. Louis, paper 98 pp. 1-10.

Vance and Siponen (2012), "IS Security Policy Violations: A Rational Choice Perspective" *Journal of Organizational and End User Computing* 24(1), pp.21-41.

Vance, A, Siponen, M. and Pahnila, S. (2012) "Motivating IS security compliance: insights from habit and protection motivation theory". *Information & Management* 49 (3–4), pp. 190–198.

Vessey, I., Ramesh, V., and Glass, R. L. (2002). "Research in Information Systems: An Empirical Study of Diversity in the Discipline and Its Journals," *Journal of Management Information Systems* 19(2), pp. 129-174.

Warkentin, Malimage and Malimage (2012), "Impact of Protection Motivation and Deterrence on IS Security Policy Compliance: A Multi- Cultural View" *pre-ICIS workshop on Information Security and Privacy* (SIGSEC). Paper 20.

Warkentin, McBride, Carter and Johnston (2012), "The Role of Individual Characteristics on Insider Abuse Intentions" *Proceedings of the Americas Conference on Information Systems (AMCIS)*, Paper 28.

Wei and Hsu (2014), "Employee Intention to Whistleblow Information Security Policy Violation" *Proceedings of the Pacific Asia Conference on Information Systems* (*PACIS*), Paper 273.

Willison and Warkentin (2013); "Beyond Deterrence: An Expanded View of Employee Computer Abuse" *MIS Quarterly* 37(1), pp.1-20.

Wolfswinkel, J.F., Furtmueller, E., and Wilderom, C.P.M. (2013), "Using Grounded Theory as a Method for Rigorously Reviewing Literature", *European Journal of Information Systems*, 22(1), pp. 45–55.