Interdisciplinary Journal of Information, Knowledge, and Management

An Official Publication of the Informing Science Institute
InformingScience.org

IJIKM.org

Volume 12, 2017

UNDERSTANDING INTERNAL INFORMATION SYSTEMS SECURITY POLICY VIOLATIONS AS PARADOXES

Kennedy Njenga* Department of Applied Information Systems, University of Johannesburg, Johannesburg, South Africa knjenga@uj.ac.za

*Corresponding author

ABSTRACT

Aim/Purpose	Violations of Information Systems (IS) security policies continue to generate great anxiety amongst many organizations that use information systems, partly because these violations are carried out by internal employees. This article addresses IS security policy violations in organizational settings, and conceptualizes and problematizes IS security violations by employees of organizations from a paradox perspective.
Background	The paradox is that internal employees are increasingly being perceived as more of a threat to the security of organizational systems than outsiders. The notion of paradox is exemplified in four organizational contexts of: belonging paradox, learning paradox, organizing paradox and performing paradox.
Methodology	A qualitative conceptual framework exemplifying how IS security violations occur as paradoxes in context to these four areas is presented at the end of this article.
Contribution	The article contributes to IS security management practice and suggests how IS security managers should be positioned to understand violations in light of this paradox perspective.
Findings	The employee generally in the process of carrying out ordinary activities using computing technology exemplifies unique tensions (or paradoxes in belonging, learning, organizing and performing) and these tensions would generally tend to lead to policy violations when an imbalance occurs.
Recommendations for Practitioners	IS security managers must be sensitive to employees tensions.
Future Research	A quantitative study, where statistical analysis could be applied to generalize findings, could be useful.
Keywords	information security, violations, paradox, systematic literature review (SLR), security policies

Accepted by Editor Rajeev Manhas | Received: August 16, 2016 | Revised: November 7, 2016; January 10, 2017 | Accepted: January 11, 2017.

Cite as: Njenga, K. (2017). Understanding internal information systems security policy violations as paradoxes. *Interdisciplinary Journal of Information, Knowledge, and Management*, *12,* Retrieved from http://www.informingscience.org/Publications/3639

INTRODUCTION

Anxiety around the security of Information Systems (IS) in many organizations has gained fundamental traction in recent years because of the threats posed by insider employees (Browne, Lang, & Golden, 2015). A primary catalyst for anxiety has been IS security incidents commonly caused by employees who are non-compliant with IS security policies. Employee non-compliance with IS security policies has been noted to lead to breaches that have cost organizations millions of dollars in losses (Herath & Rao, 2009).

Academic literature points to increased empirical studies on security compliance and violations, in an effort to understand and provide ways organizations could mitigate security threats that emanate from non-compliance of security policies by employees. An investigation of scholarly work around systems security violations points to various perspectives that would enlighten the understanding of these violations. While violation of security policies may be maliciously intended, Vroom and von Solms (2004) contend that most violations result from negligence and ignorance. Management's response to violations of negligence and ignorance is often owning up to failure in IS security governance and the programmes meant to encourage compliance.

According to Herath and Rao (2009), empirical evidence suggests that employees seldom comply with policies and moreover many allude to convenience to justify non-compliance. Deterrence theory used in IS research has suggested that unwelcome behavior and behavior that could lead to non-compliance "can be deterred through a certain, swift, and/or severe threat of punishment" (Herath & Rao, 2009). Punishment resulting from non-compliance is a central element of management decision making process and should not be seen as an easy task. It is because of such unease in decision making that many scholars have embarked on understanding inherent underlying complexities and consequences of violations (Eranova & Prashntham, 2016).

COMPLEXITIES IN UNDERSTANDING IS SECURITY POLICY VIOLATIONS

In context to the discipline of information systems, violation of security policy could be argued as inherently complex and would require a more profound understanding as to why and how security violations occur. The "problem" concerning IS security policy violations is an understanding represented in research as that of a continuum between those violations that are voluntary and malicious in nature against those that are non-voluntary and non-malicious. Nested within this continuum of security violations is a deeper but less explicit understanding of violations, in this case as 'paradoxical' and failure by research and practice to engage violations as paradoxes. Problematizing violations (critically reflecting on IS security violations) is therefore to be seen as beneficial to scholar and practice.

Scholars and practitioners in IS have attempted to problematize IS security violations and to suggest appropriate interventions from various other lenses such as neutralization (Barlow, Warkentin, Ormond, & Dennis, 2013; Siponen & Vance, 2010) and rationalization (Browne et al., 2015; Bulgurcu, Cavusoglu, & Benbasat, 2010; Vance & Siponen, 2012; Wei & Hsu, 2014). Other empirical studies on security violations have drawn on popular IS theories such as Deterrence theory (Straub, 1990), Protection Motivation (Warkentin, Malimage, & Malimage, 2012; Siponen, Mahmood, & Pahnila, 2014; Browne et al., 2015), which are seen as normative and prescriptive.

In order to better understand the theoretical predisposition of IS security policy violation, this article builds on previous published work on IS security policy violations (Njenga, 2016). What has not been explained from the said work is that these violations can be construed uniquely as paradoxes. The paradox perspective, borrowed from the discipline of management, is therefore introduced as an insightful lens in this article.

There is a limitation of scholarly work deliberating on IS security policy violations from a paradox perspective. It would therefore follow that considering IS security as paradoxes would be insightful and perhaps offer those in management practices ways to better understand and manage these viola-

tions. The purpose of this article is to therefore problematize and rationalize IS security violations from the paradox perspective. The understanding of IS security violations is revisited (Njenga, 2016) and then complemented by a distinct description of the nature and meaning surrounding paradoxes within contexts of these IS security violations. The penultimate sections problematize and present a proposed framework for understanding paradoxes in IS security discipline. The discussion, implications and conclusion follows thereafter.

IS SECURITY POLICY VIOLATION IN THEORY

Although a vast majority of organizations maintain formal written, clear, comprehensive, reasonable and well-published IS security policies (Abu-Musa, 2004), research has shown that there are violations to these policies. A systematic literature review regarding the extent to which these violations occur in organizational context was carried out by Njenga (2016) in a non-biased, replicable, scientific and rigorous way. The purpose of this review was to apply a tested and sound method of review in order to understand IS security violations within organizations (Morrell, 2008; Boell & Cecez-Kecmanovic, 2015; Khoo, Na, & Jaidka, 2011).

The use of systematic literature reviews is reaffirmed by Okoli and Schabram's, (2010) commitment to "be unaware of the need for structure in literature reviews" and to "advance policy and practice by providing the best evidence available from research" (Morrell, 2008; Atkins & Louw, 2000; Amrollahi, Ghapanchi, & Talaei-Khoei, 2013; Okoli & Schabram, 2009). There are many other ways to problematize IS security violations such as hermeneutics (Boell & Cecez-Kecmanovic, 2014), thematic analysis (Bandara, Miskon, & Fielt, 2011) or grounded theory (Wolfswinkel, Futmueller, & Wilderom, 2013). The use of systematic literature review was explained as being useful for that work because it yielded results necessary to begin to understand how IS violations have been theorized.

Njenga (2016) problematized IS security violations by extracting literature based on over 175 articles from scholarly databases in the IS discipline, such as *ACM Digital Library, Emerald Management, IEEE Xplore*, *ScienceDirect* and *ProQuest*. In addition, the *AIS eLibrary* and the *Senior Scholar Basket of Journals* were used. The search terms 'behavior', 'violation', 'security' and 'policy' were used to extract relevant articles within the domains of IS and Psychology (Chapman & Brothers, 2006). Of the 175 articles used in that work, screening was done and technical papers that did not deal with behavior were excluded (Atkins & Louw, 2000; Okoli & Schabram, 2010; Oxman, 1995). Alternative terminology (non-compliance) was also used in that work to address a well-known problem in information retrieval described as the 'indeterminacy of language' (Blair, 2006).

A backward and forward search was mentioned as having been carried out (Levy & Ellis 2006; Bandara et al., 2011; Orlikowski & Baroudi, 1991; Vessey, Ramesh, & Glass, 2002), and is revisited in Table 1.

Table 1. Search strategy

Search terms	****Search in title and 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*
*** Justification for exclusion of articles: Articles screened for methodical soundness*
**** Advanced search in title (security + policy + violation) and (non-compliance)*

CATEGORIZING IS SECURITY POLICY VIOLATION

An important outcome towards understanding IS security violations as suggested by Njenga (2016) was the disharmony on how various scholars have understood IS security violations under various contexts. Table 2 summarizes such disharmony which suggests a scholarly understanding of IS security violations existing in a continuum.

Table 2. Various categorizations of IS security policy violations (Njenga, 2016)

Authors	*Various categorizations of IS security violations by various scholars*			
Aurigemma and Mattson (2014)	*(1) malicious (intentional and deviant)*			*(2) non-malicious (volition and non-volition)*
Barlow, Warkentin, Ormond, and Dennis (2013)	*(1) malicious*	*(2) deviant behavior*		*(3) non-malicious*
Dang (2014)	*(1) intentional malicious abuse*		*(2) volitional (but not malicious noncompliance)*	*(3) non-volitional non-compliance*
Guo and Yuan (2012)	*(1) knowingly break rules (malicious)*	*(2) intentional*	*(3) involuntary*	*(4) non-malicious*
Kraemer and Carayon (2007)	*(1) violations of malicious intent*			*(2) violations of a non-malicious intent*
Martin and Imboden (2014)	*(1) intentional and malicious*		*(2) passive and non-volitional*	*(3) volitional, and non-malicious*
Siponen and Vance (2014)	*(1) deliberate violations*			*(2) non-deliberate*

EMERGENT PERSPECTIVES IN IS SECURITY POLICY VIOLATION

As Table 2 has shown, various scholars have categorized IS security violations on a continuum ranging from malicious to non-malicious violations. The categorization of IS security policy violation is seen as an important task which is deconstructed in Van Den Bergh and Njenga (2016). This conceptual categorization is as a results of a response to a call by Crossler et al. (2013) in their article titled "Future directions for behavioral information security research" who encourage scholars to try and separate and categorize various violations (such as insider employee malicious misbehavior from deviant behavior and non-malicious behavior).

Categorization of IS security policy violation is important for management practices, particularly because this would improve on the success and applicability of corrective action towards the various kinds of behavior (Crossler et al., 2013). Although it would not be the primary aim of any IS security study to just simply categorize violation behavior only, it remains important to reference such categorization and map out how effectively the categories could be balanced with the right possible deterrence effect (Loch, Carr, & Warkentin, 1992). As an example, Loch et al. (1992) have used the human perpetrator's accidental and intentional intent as part of a further study that ultimately develops a security threat taxonomy based on accidental and intentional behavior. Van Den Berg and Njenga (2016) explain the importance of using a classification schema called the 'Triad of Internal Threat Agent Behaviors' to represent the three classes of security behavior in IS security literature that would be important in enabling management to create their own threat taxonomy, based on the various types of IS security policy violations.

The idea of using a categorization of behavior to develop a threat taxonomy has been applied in the organizational context, as shown by the work of Willison and Warkentin (2013) who have focused on a holistic approach to insider computer abuse. They have considered the thought processes of human perpetrators preceding deterrence and have extended Loch et al.'s (1992) threat taxonomy, focusing on the human perpetrator (Van Den Berg & Njenga 2016). Willison and Warkentin's (2013) approach is similar and in agreement with Loch et al.'s (1992) taxonomy of behavior as intentional, but has differed on the term "accidental" violations by replacing it with the term "passive" violations.

They then proceeded to expand the taxonomy to passive non-volitional noncompliance, volitional but not malicious non-compliance, and intentional malicious computer abuse.

INTERDISCIPLINARY PERSPECTIVES IN IS SECURITY POLICY VIOLATION

In addition to various scholars categorizing IS security policy violations as a continuum of violations ranging from the extreme malicious to the unintentional and non-volitional non-malicious acts, other scholars have used other lenses from disciplines outside of IS such as sociology to explain IS security policy violations. Cheng, Li, Li, Holm, and Zhai (2013) for instance look at IS security policy violations occurring as a result of employees' weaker social bonds to their mangers, co-workers and organizations. They see this as likely leading to and influencing their willingness to engage in violations.

D'Arcy, Gupta, Tarafdar, and Ofir (2014) on the other hand have addressed the extreme end of the continuum and focus their work on those acts that exemplify the "dark side" of IT use. Their empirical studies explain that what motivates employees towards IS security policy violation is increased stress levels, work overload, interruptions and Internet addiction ultimately creating unintended consequences. They propose that these unintended violations could be moderated by sanctions and moral considerations. Kraemer and Carayon's (2007) work has involved looking at IS security violations in general from the human perspective and advocates that these violations could be as a result of human error. They see acts of procedural violations arising as a result of constructs such as forgetfulness, inattention, poor motivation, carelessness, negligence, and recklessness. Moderators to these constructs of human error would be campaigns, appeal to fear, disciplinary measures, threat of litigation and the naming, blaming and shaming approach.

From a business standpoint, Maasberg (2014) outlines the taxonomy of insider espionage as an outcome of personal crisis and disposition for civil disobedience which could lead to intellectual property theft, fraud or sabotage. Siponen and Vance (2010), in the interdisciplinary study of criminology and information systems security, present neutralization techniques that are used by employees to decrease the perceived harm of their policy violations. Ugrin and Pearson (2010) in the social sciences discipline have conducted empirical studies on cyber-loafing and the viewing and exposing others to pornography as a form of non-compliance to internal organizational policies. Warkentin, Malimage, and Malimage (2012) who base their work on criminology studies 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) empirical studies in Japanese culture suggest that violating security policy cannot necessarily be deterred through the threat of punishment.

A summary of the various theoretical aspects of IS security policy violations from many other scholars on the work of IS security violations can be drawn from Table 3 (Njenga, 2016). Table 3 shows various theoretical underpinnings used by one or more scholars to explain instances and moderations pertaining to IS security policy violations. General Deterrence Theory (GDT) is seen as the most popular theory that would explain violations with more scholars using this theoretical lens to explain violations under various contexts. In addition, Protection Motivation Theory (PMT) has also been revealed to be popular within scholarly work. An interesting approach to violation of security policies has also been suggested 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. 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 & Mattson, 2014; Bansal & Zahedi, 2015; Barlow et al., 2013; Browne et al., 2015; Cheng et al., 2013).

Table 3. Various categorizations of IS security policy violations (Njenga, 2016)

Theories used	*Systematized Literature Review Sources*	*Influences to Violating Security Policies*
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 et al. (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 et al. (2013); [3]Hovav and D'Arcy (2012); [3]Siponen and Vance (2010); [3]Takemura (2014); [3]Ugrin and Pearson (2010); [3]Warkentin et al. (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 et al. (2013)	*Individual propensity and moral belief, perceived justice of punishment, cognitive processing, moral reasoning, mandatoriness of policies*
Protection Motivation Theory	[3]Browne et al. (2015); [3]Siponen et al. (2014); [3]Warkentin et al. (2012); [3]Warkentin, McBride, Carter, and Johnston (2012); [3]Herath and Rao (2009);	*Hedonistic feelings (thrill, pleasure), intrinsic benefit Emotional state: sanctions can moderate*
Rational Choice Theory	[3]Browne et al. (2015); [3]Bulgurcu et al. (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 et al. (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 et al. (2016); [3]Cheng et al. (2013)	*Lacking in knowledge sharing, collaboration, intervention and experience leads to violations*
Involvement Theory	[3]Safa et al. (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 et al. (2014)	*Cognitively evaluate (threat and coping appraisals)*
Theory of Reasoned Action (TRA)	[3]Siponen et al. (2014)	*Attitudes and subjective norms*
General Theory of Crime	[2]Hu et al. (2014)	*Low self-control: propensity toward criminal behavior/violations*
[1]No theory Used in articles (literature)	Choi, Levy, and Anat (2012); D'Arcy et al. (2014); D'Arcy, Hovav, and Galletta (2009); Guo and Yuan (2012); Guo, Yuan, Archer, and Connelly (2011); Hu, Xu, Dinev, and Ling (2011); Hu et al. (2014); Johnston and Warkentin (2010); Kraemer and Carayon (2007); Kretzer and Mädche (2015); Maasberg (2014); Martin and Imboden (2014); Siponen and Vance (2014); Vance, Siponen, and Pahnila (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

An important consideration arising from the previous sections that have addressed various perspectives of scholarly work on IS security policy violation is the omission of the paradox perspective to problematize IS security violations. The next section suggests how the paradox perspective could be used to problematize such violations in useful and insightful ways.

PARADOXES IN PRACTICE

According to Eranova and Prashntham (2016), paradoxes are "elements that seem logical in isolation but absurd and irrational when appearing simultaneously". These social constructs are seen as both logical and absurd. Understanding paradoxes has appealed to management research literature (Smith & Lewis, 2011; Smith & Tushman, 2005) because of the influence it has on models for decision making (Robison, Shupp, & Myers, 2010). Rooted in Management discipline regarding paradox is work by Smith and Lewis (2011) who explain the paradox perspective in management. The paradox paradigm would be an important perspective to consider in the context of IS security policy violations since it offers an alternative to other previously held paradigms (such as neutralization and rationalization explained in earlier sections) in the IS discipline. The paradox perspective holds on to the idea that confirming opposing forces can be useful in understanding complex and dynamic environments (Eranova & Prashntham, 2016). In IS security literature, this is important because of the various tensions that exist between the practice of using people as part of the control systems (distinctly and at the same time collectively) while simultaneously strengthening system controls from the same people who run these systems. This aspect is seen as problematic. Tension is problematized as follows; organizations do need people but at the same time it is those very people who pose a bigger risk to these organizations. Indeed, tensions are key to identifying and understanding organizational paradoxes particularly in IS security domains because of a "tug-of-war between opposing forces" of security controls and people (Andriopoulos & Lewis, 2010). It is important to understand tension within the IS security domain because in security matters, there are inherent contradictions and inconsistencies. One such contradiction is that of attempting to restrict security access to information resources while simultaneously advocating for performance. The simultaneous presence of opposites (access and restricted use) becomes part of an everyday information security concern. Failure and tension is therefore revealed by the numerous IS security violations and breaches reported.

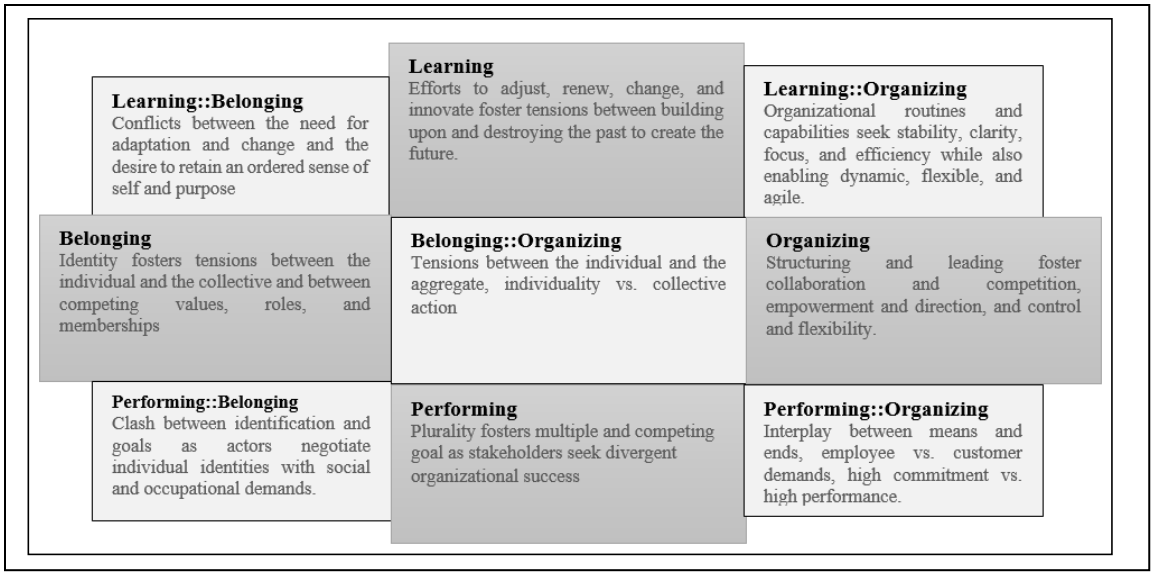

Figure 1: Paradox framework (Smith & Lewis, 2011)

Organizational paradoxes and tensions are well documented by Smith and Lewis's (2011) work which is based on a sample of 360 journal articles, survey over 12 years across 12 management journals. A

synthesis of literature is carried out through a paradox framework which categorizes paradoxes across four areas of; belonging, learning, organizing and per-forming. This is shown by Figure 1.

The four categories of paradox identified in Figure 1, and applicable to the IS security management domain, represent the core management activities within organizational settings. According to Smith and Lewis (2011), the *learning paradox* is characterized by the tensions in the shaping of new and destroying of old systems. The *belonging paradox* is characterized by the tensions of the individual against the collective where employees are likely to face opposing yet co-existing roles. The *organizational paradox* is characterized by the tensions of routine *vis-à-vis* change and of collaboration, *vis-à-vis* competition. The *performing paradox* is characterized by the tension of differing and conflicting demands of various stakeholders.

THE PARADOX PERSPECTIVE IN IS SECURITY POLICY VIOLATION

LEARNING PARADOX: TENSIONS TOWARDS IS SECURITY POLICY VIOLATIONS

Within IS security practices, there are continuous efforts to renew, change, and innovate, which are seen as paramount for sustainable IS security initiatives. This is because of the emergent nature of security threats such as new viruses, new worms, new malware and new sets of risks associated with evolving hacking attacks. Mitigating against these security risks must be done against the background of destroying old practices and systems. The destruction of the old and reinventing new systems is seen as a security practices that will ultimately create tensions.

An important new and emerging system change is the growing use and introduction of mobile devices into organizational spaces and shared networks which has created new security concerns. If these devices are lost or stolen as a result of negligence on the part of the employees, potentially sensitive organizational data residing in these devices maybe accessed by unauthorized users (Martin & Imboden, 2014). This use of mobile devices will create opportunities for learning. An interesting learning paradox is the extent to which organizations address such challenges posed to IS security practitioners on whether or not to allow or restrict the use of these devices. Emotional displeasure and tensions are bound to occur on either choice of use. Bansal and Zahedi (2015) in their use of Attribution theory talk of emotional displeasures that result from changes in ways people have previously interacted with systems and this often becoming a cause for violations of these systems. The paradox is that unavoidably, change must happen, but change is not pleasurable.

BELONGING PARADOX: TENSIONS TOWARDS IS SECURITY POLICY VIOLATIONS

The idea of belonging can be explained using social science theories such as Social bond theory (SBT) used by scholars in IS security research to explain deviance (Safa et al., 2016). Deviance towards IS security policies occurs when the social bond (and lack of belonging) is perceived as weak from an employee's perspective. If for instance it is perceived that attachment, involvement and commitment to these systems is limited, and that employees do not see themselves as part of the system, their tendency to violate IS security policies increases correspondingly.

Different and competing roles that forces employees to fluctuate between acting as a collective units or acting as individuals create a belonging paradox which is ultimately characterized by violations. Almusharraf et al. (2015) have used the Personal Construct Theory to explain these tensions and suggest that insufficient understanding or roles and duties, policies and structures anchored on different personal constructs create tensions in responsibilities, ownership and role.

As an example, IS security policy that deal with privacy is underscored by tensions of belonging, since people could be inclined to share organizational information in order to have a sense of belonging to that organization , while on the same breath strongly object to the very organization's uncontrolled use of personal their data (Kokolakis, 2015).

Performing Paradox: Tensions Towards IS Security Policy Violations

There are various stakeholders in the development, implementation and enforcing IS security policies. The plurality and attrition of performance amongst these stakeholders often causes competing goals, as each seeks success in performance from their own perspectives. IT security developers see completeness and complexities of security controls from technical perspectives, while IT managers are much more motivated towards ideals of protective measure to deter and prevent system abuse from the softer qualitative managerial perspectives. An apparent paradox and contradiction is presented in the form of competing goals such as softer qualitative goals *vis-a-vis* technical quantitative performance goals (Das & Teng, 2000). A paradox of performance in this instance can manifest when the level of involvement and commitment leading to performance and adherence to security policies is shaped by the qualitative aspects of attitude (short-term personal gain verses long term personal gain). Involvement Theory discusses the level of energy, time and participation in a particular activity and has been used by IS researcher to explain violations (Safa et al., 2016).

Organizing Paradox: Tensions Towards IS Security Policy Violations

IS security practitioners and employees work within organizational structures that foster competition and cooperation simultaneously resulting in various tensions. According to Das and Teng (2000) while cooperation ultimately seeks value creation, seen as a positive-sum game with shared benefits, conversely competition demands opportunistic behavior and is seen as a zero-sum game and that the benefits accrued are personal. The framework shown by Figure 2 presents a summary of these four paradox perspectives within these IS security contexts and which problematizes IS security policy violations as Paradoxes.

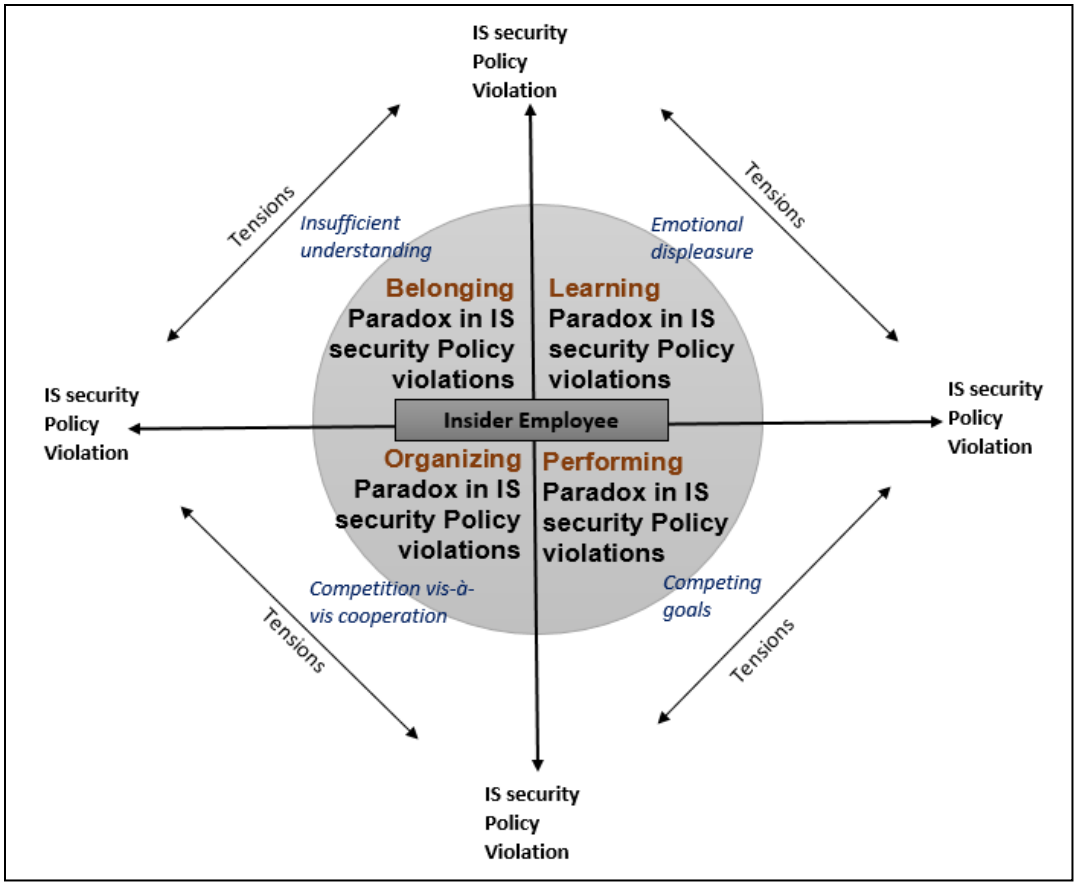

Figure 2: Problematizing IS security violations as a Paradox violations

DISCUSSION

Problematizing IS security policy violations as paradoxes is indeed an insightful way of appreciating how violations of IS security policies occur. Context is elucidated from an 'either/or' framework that envisages two opposites as mutually independent with only one of the two operating at a given time. The employee generally in the process of carrying out ordinary activities using computing technology exemplifies unique tensions (or paradoxes in belonging, learning, organizing and performing) and these tensions would generally tend to lead to policy violations when an imbalance occurs. This is an interesting perspective that IS security literature has not considered before. Such a perspective offers an opportunity for managers to understand that an imbalance surrounding an employee's inability to manage their need of belonging, learning, organizing and performing on the context of adhering to security policies will make it possible for the employee to be perceived as more of a threat to the security of an organization systems as opposed to an outsider. This suggestion is backed up by Barlow et al. (2013), where they present data from a survey that shows that 80 percent of chief information security officers (CISOs) believe that employees present a greater threat to their data than external hackers.

Understanding the framework presented in Figure 2 which problematizes IS security policy violations as paradoxes is one step closer towards enabling better decisions being made by managers regarding how to remedy these IS security violations. Indeed the paradox management approach invites managers to continuously adjust decisions and actions by appreciating the tensions and conflicting pressures employees face. This idea is compelling and also compatible with the findings of Ricciardi, Zardini, and Rossignoli (2016), who confirm that paradoxical dimensions of organizational dynamism enable adaptive regeneration of various models. IS security policy formulation and policy management could be seen as one such model where dynamism and adaptive regeneration is to be encouraged.

IMPLICATIONS AND RECOMMENDATIONS FOR IS SECURITY MANAGEMENT

From an understanding of Figure 2 framework above, and the discussions thereon, it remains very possible for IS security managers to harness paradoxical tensions as conduits to IS security innovation and adaptive regeneration (Ricciardi et al., 2016). While it is discerning that IS security policy violations could be construed as paradoxes characterized by contradictory propositions, the important thing to note is that IS security managers do not necessarily have to address or make a choice between these contradictions. This may seem radical at first but, importantly, Smith and Lewis (2011) argue that it is possible to "generate responses that embrace the tensions and synergise the opposing propositions". This they argue presents management with the opportunity to: (1) push conceptual and cognitive limitations and (2) spark sense-making and creative thinking, which in turn can lead to flexibility and fluidity (Smith & Lewis, 2011, as cited by Tse, 2013). What this means to the IS security domain is that while the employee is to be seen as a threat to the organization (when they violate IS security policies, they should paradoxically be also be equally and uniquely seen as the solutions to IS security threats, while also being co-creators of such policies. The following recommendations are suggested in line with understanding violation paradoxes.

1. IS security managers must be sensitive to employees tensions leading to violations which could arise from emotional displeasure, insufficient understanding about tasks, competing goals as well as when employees compete and cooperate with each other. Rather than focusing on tensions/contradictions from an 'either/or' perspective, such that there is a solution for every one side of a problem, managers must value both sides of tensions and embrace a 'both/and' perspective, that synergizes opposing perspectives. Formal reporting of tensions is to be encouraged.
2. Mangers must learn about how to detect early warning signs arising from tensions. A record must be kept of these early warning signs leading to IS security violations and records must be

mapped against an agreed threat taxonomy to the organization. IS security managers should cultivate a culture of recording and acknowledging accomplishment of tasks that mitigate threats as a first step in addressing organizational tensions. They should understand that employees are valuable assets to organizations and that their needs and actions also matter. They should consider their own perspectives as well as employee perspectives as complementary and additives, such that when IS security policy violations occur and are recorded, these should be seen as unique opportunities for learning.

SUGGESTIONS FOR FUTURE WORK

This work has been both descriptive and analytical while covering important scientific literature regarding internal IS security policy violations. The paradox perspective, which considers IS security policy violations from multiple disciplines, has been conceptualized. It would be useful to build further on this work by incorporating the paradox perspective as an important theoretical lens in the discipline of information systems security and to empirically test this across various regions in the world. A quantitative study, where statistical analysis could be applied to generalize findings could be useful for this purpose.

CONCLUSION

This article has placed context to organizations where high levels of anxiety is faced by managers due to increased IS security policy violations. The complexities on how to manage these violations have been presented and explained. There has been a lot of interest and empirical work done regarding IS security policy violations as show by the systematic literature review presented in the first sections of this article. The need to understand what literature says around IS security policy violations and to problematize these violations (as paradoxes) as shown by the other sections of this work is not only important but timely. This is true considering that the study of IS security violations continues to receive a great deal of attention in IS literature.

The article ends by suggesting an insightful perspective regarding IS security policy violations that are to be construed uniquely as paradoxes. Specific recommendations that could mitigate organizational tensions are presented. The paradox framework for IS security policy violations has been presented as a way to guide management on how to effectively intervene. What this means to IS security management is that it is still possible for them to harness paradoxical tensions as conduits to technology (security) innovation rather than try to hinder these. A much broader study embarking on more qualitative and systematic studies that touch on paradoxical tensions in many other IS security activities is also encouraged. Such a study would further the understanding of various undertakings within the domain of information systems security.

DECLARATION

The work is derived from published work (Njenga, 2016) that explains the systematic literature review (SLR) process used to conceptualize IS security policy violations. This work complements while delving deeper into the aspects of IS security policy violations from the paradox perspective in insightful and different ways from previous work. The paradox perspective has not been considered before in IS security literature and it would be important for both general management of organizations and Information Systems Security scholars and practitioners to recognize that there are insightful ways drawn from management discipline that would add meaning towards how IS security violations are perceived. Publication of this work would therefore be significant for this to be realized.

REFERENCES

Abu-Musa, A. A. (2004). Investigating the security policies of computerized accounting information systems in the banking industry of an emerging economy: The case of Egypt. *The Review of Business Information Systems, 8*(3), 83-102.

Almusharraf, A., Dhillon G., & Samonas, S. (2015). Mismatched understanding of IS Security Policy: A RepGrid analysis. *Proceedings of the 21st Americas Conference on Information Systems (AMCIS)*, Puerto Rico.

Amrollahi, A., Ghapanchi, A. H., & 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), 39–66.

Andriopoulos, C., & Lewis, M. W. (2010). Managing innovation paradoxes: Ambidexterity lessons from leading product design companies. *Long Range Planning, 43*(1), 104-122.

Atkins, C., & Louw, G. (2000). Reclaiming knowledge: A case for evidence based information systems reclaiming knowledge. *Proceedings of the 8th European Conference on Information Systems (ECIS),* Vienna, Austria.

Aurigemma, S., & 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.

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)*, Helsinki, Finland.

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

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

Blair, D. (2006). *Wittgenstein, language and information. Back to the rough ground!* Dordrecht: Springer.

Boell, S. K., & Cecez-Kecmanovic, D. (2014). A hermeneutic approach for conducting literature reviews and literature searches. *Communications of the Association for Information Systems, 34*(12), 257-286.

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

Browne, S., Lang M., & 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),* Münster, Germany.

Brunel, J., Cuppens, F., Cuppens, N., Sans, T., & Bodeveix, J. P. (2007). Security policy compliance with violation management, *Proceedings of the ACM Workshop on Formal Methods in Security Engineering,* 31-40.

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

Chapman, B., & Brothers, P. (2006). Database coverage for research in management information systems, *College & Research Libraries,* 67(1), 50-62. DOI: 10.5860/crl.67.1.50.

Chang, K-C., & Seow, Y. M. (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.

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

Choi, M., Levy Y., & 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., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*(1), 90-101.

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)*. Paper 10.

D'Arcy, J., Gupta, A., Tarafdar, M., & Ofir, T. (2014). Reflecting on the "dark side" of information technology use. *Communications of the Association for Information Systems, 35*(5), 109-118.

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.

Das, T. K., & Teng, B. S. (2000). Instabilities of strategic alliances: an internal tensions perspective, *Organization Science, 11*(1), 77–101.

Eranova M., & Prashntham, S. (2016). Decision making and paradox: Why study China? *European Management Journal, 34*(3), 193-201.

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model, *Information & Management,* 49(6), 320–326.

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

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

Hovav, A., & 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), 99-110.

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.

Hu, Q., West, R., & Smarandescu, L. (2014). The role of self-control in information security violations: Insights from a cognitive neuroscience perspective, *Journal of Management Information Systems, 31*(4), 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) 69-79.

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

Kokolakis, S. (2015). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security,* doi: 10.1016/j.cose.2015.07.002.

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

Kretzer, M., & 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, TX, 1-17.

Khoo, C. S. G., Na, J.-C., & Jaidka, K. (2011). Analysis of the macro-level discourse structure of literature reviews. *Online Information Review, 35*(2), 255-271.

Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science Journal*, *9*, 181-212. Retrieved from http://inform.nu/Articles/Vol9/V9p181-212Levy99.pdf.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly, June,* 173-186.

Maasberg, M. (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.

Martin, N. L. & 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.

Molok, A., Ahmad, A., & 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, Qld.

Morrell, K. (2008). The narrative of 'evidence based' management: A polemic. *Journal of Management Studies 45*(3), 613-635.

Njenga, K. (2016). Information systems security policy violation: Systematic literature review on behavior threats by internal agents. *Proceedings of the International Conference On Information Re-sources Management (Conf-IRM),* Cape Town, South Africa.

Okoli, C., & Schabram, K. (2009). Protocol for a systematic literature review of research on the Wikipedia. *Sprouts: Working Papers on Information Systems, 9*(65).

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research. *Sprouts: Working Papers on Information Systems, 10*(26).

Orlikowski, W. J. & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions, *Information Systems Research*, *2*(1), 1-8.

Oxman, A. D. (1995). Checklists for review articles. In I. Chalmers & D. G. Altman (Eds.), *Systematic reviews* (pp. 75-85). London: BMJ.

Ricciardi, F., Zardini, A., & Rossignoli, C. (2016). Organizational dynamism and adaptive business model innovation: The triple paradox configuration, *Journal of Business Research*. Retrieved from http://dx.doi.org/10.1016/j.jbusres.2016.04.154

Robison, L. J., Shupp, R. S., & Myers, R. J. (2010). Expected utility paradoxes. *The Journal of Socio-Economics, 39*(2), 187-193.

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

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487-502.

Siponen, M. & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. *European Journal of Information Systems, 23*, 289-305.

Siponen, M., Mahmood, M. A. & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224.

Smith, W. K., & Lewis, M. W. (2011). Toward a theory of paradox: a dynamic equilibrium model of organizing, *Academy of Management Review, 36*(2), 381-403.

Smith, W. K., & Tushman, W. L. (2005). Managing strategic contradictions: A top management model for managing innovation streams. *Organization Science, 16*(5), 522-536.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.

Takemura, T. (2014). Empirical analysis of intentional security policy violation in the workplace. *Economic Review, 46*(6), 21-40.

Tse, T. (2013). Paradox resolution: A means to achieve strategic innovation, *European Management Journal*, *31*, 682-696.

Ugrin, J. C., & 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, MO. Paper 98.

Van Den Bergh, M., & Njenga, K. (2016). Information security policy violation: The triad of internal threat agent behaviors. *Proceedings of the 1st International Conference on the Internet, Cyber Security, and Information Systems (ICICIS),* Gaborone, Botswana.

Vance, A. & Siponen, M. (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing, 24*(1), 21-41.

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

Vessey, I., Ramesh, V., & 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), 129-174.

Vroom C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198.

Warkentin, M., Malimage, N. & Malimage, K. (2012). Impact of protection motivation and deterrence on IS security policy compliance: A multicultural view. *Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)*. Paper 20.

Warkentin, M., McBride, M., Carter, L., & Johnston, A. (2012). The role of individual characteristics on insider abuse intentions. *Proceedings of the Americas Conference on Information Systems (AMCIS),* Paper 28.

Wei, L. C., & Hsu, C. (2014). Employee intention to whistleblow information security policy violation. *Proceedings of the Pacific Asia Conference on Information Systems (PACIS),* Paper 273.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse, *MIS Quarterly, 37*(1), 1-20.

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. M. (2013). Using grounded theory as a method for rigorously reviewing literature, *European Journal of Information Systems, 22*(1), 45-55.

BIOGRAPHY

Kennedy Njenga, PhD, is a senior faculty member at the Department of Applied Information Systems, University of Johannesburg in South Africa. He has published and presented his research both nationally and internationally in the field of information systems security. His research focuses on methodological and philosophical issues related to security of information systems such as deviant computer behavior. He also has a special research interest on security around the use of wireless and mobile applications in organizations.