Journal of Knowledge Management Application and Practice
An International Journal

http://dx.doi.org/10.18576/jkmap/020205

Knowledge Sharing and Information Security: A Conflict of Interest?

Ghosia Ahmad[*]

Sun Yat-Sen University, Guangzhou, Guangdong Province, China.

Received: 10 May 2020, Revised: 27 Jun 2020, Accepted: 23 Jul. 2020.
Published online: 1 Aug 2020.

Abstract: The purpose of this paper is to explore the paradoxical and concurrent nature of knowledge sharing and information security and address an important yet predominantly overlooked research gap in the middle-ground between the disciplines of knowledge management and information security.
Firstly, relevant knowledge sharing literature is reviewed, establishing how it is defined, what the most common human, organisational and technological factors influencing this practice are, the acts of knowledge hiding and knowledge hoarding and the role of knowledge protection in relation to knowledge sharing. Secondly, information security literature is reviewed, determining how the concept is defined, what the most common human, organisational and technological information security threats and subsequent protection measures are. Finally, literature on knowledge sharing and information security is synthesized to draw attention to their middle-ground, investigate the relationship and highlight their inherently conflicting aims and present the research gap.

By reviewing the literature on knowledge sharing and information security, particularly, by exploring their relationship, an inherent conflict and research gap has been identified. Further, knowledge management literature has focused on facilitation of knowledge sharing and overlooked knowledge protection, whereas information security has focused primarily on technical aspects and protecting 'information' and explicit knowledge, and subsequently neglected the development of more holistic approaches that include tacit knowledge protection. Although, some researchers have highlighted concerns regarding the conflict and aimed to explore the area of knowledge protection, the level of overall research on this topic in knowledge sharing literature, or in the wider discipline of knowledge management, is sparse. Further, due to the lack of empirical research on the issue, there is a lack of guidance for organisations about managing the conflict, protecting sensitive 'knowledge' and broadening their KM strategy and aligning it consciously with information security practices.

There is a subsequent need for empirical studies to identify the ways the conflict can manifest itself in different organizational settings and development of guidelines based on these.

This paper simultaneously explores and bridges the disciplines of knowledge management and information security and by focusing on their concurrent nature and middle-ground and highlights the inherent conflict between knowledge sharing and information security practices. The research gap is elicited using a holistic and informed approach by presenting a set of assumptions drawn from pervious literature from both disciplines.

Keywords:. Management, Knowledge Sharing, Information Security, Knowledge Protection.

1 Introduction

This research bridges the disciplines of knowledge management and information security by exploring the conflict between knowledge sharing and information security practices.
By reviewing the literature on knowledge sharing and information security, and more importantly, by exploring the relationship between the two practices, an inherent conflict has been identified (e.g. Desouza, 2006; Shedden et al, 2011; Ahmad et al, 2014; Manhart and Thalmann, 2015; Ilvonen et al, 2016). The conflict is caused by their intrinsically

[*] Corresponding author e-mail: ghosia_ahmed@yahoo.co.uk

opposing goals; knowledge sharing aims to encourage individuals to share knowledge with colleagues, organisational partners and suppliers; on the other hand, information security initiatives aim to apply controls and restrictions to the knowledge that can be shared and how it is shared.
Knowledge management has focused on facilitation of knowledge sharing and overlooked knowledge protection, whereas information security has focused primarily on technical aspects and protecting 'information' and 'data', and subsequently neglected the development of more holistic approaches that also include the protection of knowledge (Manhart and Thalmann, 2015). The limited previous research on this issue of knowledge protection (e.g. Ilvonen et al, 2016; Manhart and Thalmann, 2015; Shedden et al, 2011; Desouza, 2006), has predominantly been of a conceptual nature, has been biased towards the aim to improve protection of knowledge and has typically been grounded in the knowledge management domain. This surfaces a gap (Figure 1) for further research that takes a holistic and unbiased approach to exploring the practices of knowledge sharing and information security, focusing on their middle-ground and identifying ways their concurrent nature conflicts.

2 Literature Review

2.1 Knowledge Sharing

In fast-changing environments where there is a great need to "understand customers' demands and competitors' strategies" (Lin et al, 2012: 42), knowledge is a vital strategic and competitive resource for organisational success (Martelo-Landroguez and Cepeda-Carrión, 2016), and subsequently, an increasing amount of attention has been given to knowledge management (KM) in academic research (Heisig et al, 2016). According to Martelo-Landroguez and Cepeda-Carrión (2016) the four key processes for achieving this success through KM are identified in the literature as (i) knowledge creation, (ii) knowledge transfer/sharing, (iii) knowledge storage/retrieval and (iv) knowledge application. Whereas, based on a comparison of 160 knowledge management frameworks from around the world and their respective activities for systematically handling knowledge resources, Heisig (2009: 13) concludes that the "result of the analysis shows that there are five most frequently mentioned broad categories of KM activities: share, create, apply, store and identify knowledge".
Knowledge sharing in particular has been recognised as an integral activity for organisational success (e.g. see Dyer and Nobeoka, 2000; Wasko and Faraj, 2005; Renzl, 2008) and has been receiving increasing attention in both research and practice (Yi, 2015; Fullwood et al, 2013). "A fundamental component of both KM and learning is the concept of knowledge sharing" (Chinowsky and Carrillo, 2007: 127), and according to Wang and Noe (2010) and Stenius et al (2016), KM's success is dependent on knowledge sharing. Furthermore, Stenius et al (2016: 181) describe knowledge sharing as a critical behaviour in a knowledge-based organisation as such an organisation is "reliant on effective utilization of its collective knowledge pool, particularly its knowledgeable employees".
Whilst a unanimous definition of knowledge sharing does not appear to exist as researchers often define knowledge sharing from their personal or research contextual point of view (Wu and Zhu, 2012), by drawing on existing literature and analysing the various definitions of knowledge sharing identified, in this paper the following five common aspects have been identified in relation to what constitutes knowledge sharing for the said theorists:

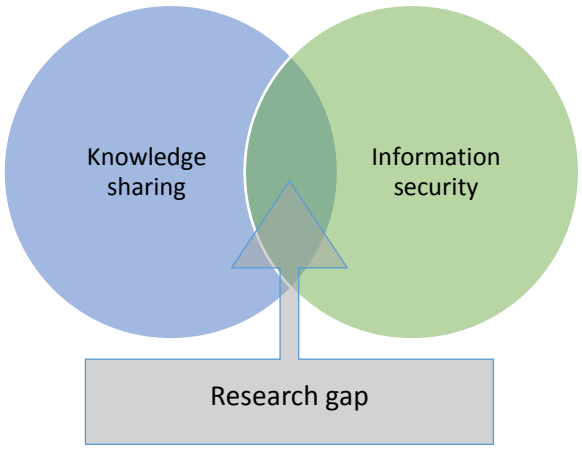

Fig. 1**:** Middle-ground between njhbjhv sharing and information security.

I. making use of or exploiting the already existing knowledge within the organisation (e.g. Jackson et al, 2006; Christensen, 2007; Chinowsky and Carrillo, 2007; Raab et al, 2014; Stenius et al, 2016),

II. sharing the knowledge from one person or source to another (Gibbert and Krause, 2002; Levin and Cross, 2004; van den Hooff and de Ridder, 2004; Jackson et al, 2006; Christensen, 2007; Haas and Hansen, 2007; Chinowsky and Carrillo, 2007; Stenius et al, 2016),
III. applying the knowledge to tasks or solving problems (Grant, 1996; Christensen, 2007; Raab et al, 2014; Stenius et al, 2016),
IV. contributing to individual and organisational learning (Huysman and De Wit, 2002; Hansen, 2002; Goffin and Koners, 2011; Park and Lee, 2014; Heisig et al, 2016),
V. contributing to performance or innovation (Huysman and De Wit, 2002; Hansen, 2002; Jackson et al, 2006; Park and Lee, 2014; Heisig et al, 2016).

Drawing upon these definitions offered by other researchers, and by summarising and identifying the core components, knowledge sharing is defined in this paper as:
The process of identifying and communicating existing tacit or explicit knowledge through any means – i.e. direct human interaction, documented or electronically - from one entity to another for the purpose of generating learning, reciprocity, completing a task, solving a problem or generating improvement. The 'entity' may be an individual, a group, an organisation or a system.

2.1.1 Factors that Influence Knowledge Sharing

Many organisations make it a priority to identify factors that will motivate their employees to share knowledge. Based on previous literature (Wu and Zhu, 2012). Riege (2005) identified three categories of factors that form barriers to knowledge sharing, that include individual factors (e.g. lack of trust, fear of loss of power, and lack of social network), organisational factors (e.g. lack of leadership, lack of appropriate reward system, and lack of sharing opportunities), and technological factors (e.g. inappropriate information technology systems and lack of training).
In this paper, we draw upon existing literature to identify the following human, organisational and technological factors that that have been found to motivate or hinder knowledge sharing. The factors identified include social connection, trust, perceived benefits, support from management and the use of technologies. In addition, the issues of knowledge hiding and hoarding and the importance of knowledge protection will also be discussed.

2.1.1.1 Human

Social Connections

Social connection with the knowledge receiver is likely to motivate the knowledge owner to share knowledge (Reagans and McEvily, 2003) and according to Raab et al (2014), it is strong social ties that support complex knowledge sharing and facilitate effective knowledge dissemination, particularly individual-level knowledge sharing which requires common ground for understanding to enable all the individuals involved to extract what they find useful.

Trust

Knowledge sharing behaviour is more likely to be influenced by intrinsic factors such as trust, gratitude and personal obligation (Fullwood et al, 2013). As trust is one of the fundamental principles of an effective social exchange between individuals (Blau, 1964), when looking at knowledge sharing from a human behaviour perspective, the role of trust has been recognised as an important element by various researchers (e.g. Pillai et al, 1999; Wasko and Faraj, 2005; Ritala et al, 2015). A knowledge requester needs trust in the knowledge provider to ensure that the knowledge provided is accurate and helpful, and, the knowledge provider must trust the knowledge receiver to handle and use the knowledge appropriately (Staples and Webster, 2008). Similarly, a lack of trust between the knowledge provider and receiver becomes a barrier to knowledge sharing (Levin and Cross, 2004; Bakker et al, 2006).

Perceived Benefits

"Perceived rewards have been shown to have a significant effect on many work behaviours", including, knowledge sharing (Cabrera et al, 2006: 250-251). Sedighi et al (2016) argue that knowledge sharing incentives have typically been of a psychosocial and intangible nature in accordance with social exchange theory where individuals voluntarily engage in activities if the benefits are perceived to be greater than the costs. Further, based on social exchange theory, self-interest drives people's actions thus the motivation behind knowledge sharing is the expectation of reciprocation (Serenko and Bontis, 2016).
Whilst some studies have identified the benefits of monetary rewards for more formal and measurable types of knowledge sharing (e.g. Bartol and Srivastava, 2002) and others congruently argue that a lack of incentives can be a knowledge sharing barrier (Yao et al, 2007), payment rewards based on performance can discourage knowledge sharing (Huber, 2001)

and formal initiatives such as extrinsic reward systems may have a counter-effect on existing intrinsic knowledge sharing behaviours and motivations (Osterloh and Frey, 2000; Robertson and Swan, 2003).

2.1.1.2 Organisational Leadership

Employees are willing to share knowledge if this behaviour is desirable and expected by management (Martiny, 1998); "employees are interested in acting in accordance with management direction", thus, management's commitment creates a more positive knowledge sharing culture (Connelly and Kelloway, 2003: 298). Donate and Pablo (2015) also found that knowledge-oriented leadership contributed to improved knowledge sharing by integrating disparate KM practices.
Equally, Riege (2005) asserts that a lack of support, communication and direction from management can be a barrier to knowledge sharing. Raab et al (2014), however, argue that whilst management involvement can reduce cultural barriers to knowledge sharing, it may not necessarily contribute to nurturing of trust - a necessary prerequisite for effective knowledge sharing, particularly concerning tacit knowledge.

Organisational Culture

Organisational culture plays an important role in nurturing knowledge sharing (e.g. Davenport and Prusak, 1998; McDermott and O'Dell, 2001; Riege, 2005; Wang and Noe, 2010; Islam et al, 2015; Ni et al, 2016) it is therefore important to take it into account when designing knowledge sharing strategies (Fullwood et al, 2013).
Organisational culture becomes a barrier when it does not provide the necessary support for knowledge sharing, however, efforts to adjust organisational culture to fit KM strategies also hinder knowledge sharing (Riege, 2005). Cultural barriers arise from the way KM is designed and implemented, rather than the culture itself (McDermott and O'Dell, 2001). Thus, instead of trying to change it, KM can be used to inform and influence organisational culture (Liebowitz, 2008) providing that it matches the core values and style of the organisation and is built around existing knowledge sharing networks (McDermott and O'Dell, 2001).

2.1.1.3 Technological

Technologies and Systems

Organisations demand instant knowledge access and availability for various stakeholders (Davison et al, 2013) and to reduce obstacles such as chronological, social and physical distances and create new motivation for the users to share knowledge (Hendriks, 1999). Knowledge management systems (KMS) are information systems implemented for managing organisational knowledge with the aim to improve the way knowledge is created, stored, transferred and applied and thus enabling knowledge sharing through capturing individual knowledge and disseminating it widely (Santoro et al, 2017).

In recent years, new knowledge sharing possibilities arise through the emergence of 'The Internet Of things' (IoT), "the concept of connecting any device with an on-and-off switch to the Internet and or to each other" whereby data is collected and transmitted (Attaran, 2017: 10). The IoT is a model based on the concept that "Anything that can be connected, will be connected" (Morgan, 2014); it is changing the nature of innovation through disruptive technologies and creating new possibilities through digital ecosystems for organisations to gather and share knowledge (Santoro et al, 2017).

It is also recognised that technology may not breakdown all human or geographic barriers to knowledge sharing (Babcock, 2004), thus, its role should be that of an enabler, rather than a driver (Martiny, 1998). Knowledge sharing may be hindered if the systems and processes are not well-integrated, there is insufficient technical support, a gap between the users' needs or expectations and the technology's capability, the system being limited to only managing the 'existing' knowledge, or a lack of understanding, familiarity and training (Riege, 2005; Davison et al, 2013). Further, a significant amount of organisational knowledge is in tacit form which cannot be fully converted into explicit knowledge for technological systems whilst preserving its contextual richness (Davison et al, 2013).

2.1.2 Knowledge Hiding and Hoarding

The concepts of 'knowledge hiding' or 'knowledge hoarding' have also been recognised as possible barriers to knowledge sharing (e.g. Davenport and Prusak, 1998; Hislop, 2003; Connelly et al, 2011; Serenko and Bontis, 2016).

Connelly et al (2011: 65) define 'knowledge hiding' as "an intentional attempt by an individual to withhold or conceal knowledge that has been requested by another person". Further, Connelly et al (2011) also highlight that knowledge hiding and a lack of knowledge sharing are dissimilar behaviours and underpinned by very different motivations. "Knowledge hiding might be motivated by a number of different reasons (e.g., prosocial, instrumental, laziness, etc.), whereas a lack of knowledge sharing is likely only driven by an absence of the knowledge itself." (Connelly et al, 2011: 67). Moreover, Serenko and Bontis (2016: 1199) also stress that "knowledge hiding and knowledge sharing belong to unique yet possibly overlapping constructs". As per the social exchange theory discussed earlier, reciprocation affects knowledge sharing

behaviour (Hall et al, 2010), which means that negative actions, such as intentional knowledge hiding, may equally be reciprocated (Serenko and Bontis, 2016). Having a positive organisational knowledge culture can reduce knowledge hiding behaviours (Serenko and Bontis, 2016).

'Knowledge hoarding' on the other hand, is when an individual accumulates knowledge that may or may not be shared in the future (Hislop, 2003; Evans et al, 2015). Whilst both concepts "can be characterised as a repertoire of possible behaviours that can be classified as withholding knowledge" (Connelly et al, 2011: 66-67), the key difference is that in 'knowledge hiding' an individual intentionally conceals knowledge requested by another individual, whereas 'knowledge hoarding' is the accumulation of knowledge not necessarily requested to be shared.

2.1.3 Knowledge Protection

Knowledge is a source of competitive advantage and is valuable to the organisation when shared (Raab et al, 2014; Alavi and Leidner, 1999), equally, it is important to protect valuable knowledge from illegal or inappropriate theft (Gold et al, 2001). Despite knowledge sharing having been widely recognised as an integral part of KM, knowledge protection has not received the same level of attention (Ilvonen et al, 2016). Desouza and Awazu (2004: 22) argue that "organisations are naïve in their attempts to secure their most valuable resource: knowledge". Securing knowledge should occur at three levels: 'product', 'process' and 'people' (Desouza, 2006; Desouza and Vanapalli, 2005). However, unlike explicit knowledge or 'information' that can be protected through information security measures, protecting tacit knowledge is a challenge due to its invisible and 'flux' nature (Desouza, 2006).

Scarcity of literature and research on knowledge protection is noted, particularly in the years prior to 2010 where some of the studies identified include protection strategies for preventing knowledge spillovers (De Faria and Sofka, 2010), knowledge protection in strategic alliances (Norman, 2004) and intellectual property rights (Zhao, 2006). Despite the scarcity of knowledge protection literature in previous years (e.g. Shedden et al, 2011; Manhart and Thalmann, 2015; Ilvonen et al, 2016), knowledge protection and its integral role in knowledge management is starting to gain more attention in recent years. Vayrynen et al (2013) explored knowledge protection challenges of social media for organisations, Ahmad et al (2014) studied organisational knowledge protection strategies in organisations in the interest of competitive advantage and preventing leakage, and Manhart and Thalmann (2015) investigated relevant literature on knowledge protection and highlighted its scarcity. Ilvonen et al (2016) also explored the contradictory nature of knowledge sharing and protection in various organisations in Finland.

2.2 Information Security

Information security is a globally recognised discipline (Gifford, 2009) and is one of various requirements of an employee's or employer's working day (Albrechtsen, 2007). The purpose of information security is to protect the valuable information resources of an organisation through the application of appropriate policies, standards and procedures as part of the complete information security program that supports the organisation to meet its business objectives (Peltier, 2016).

There exist differences in the definitions, purpose and adoption of information security by different researchers. Information security is far-reaching and involves various approaches that attempt to protect valuable information assets and mitigate threats (Crossler et al, 2013). According to Winkler (2011) information security consists of the management of loss of information and its resulting cost. However, a more common definition of information security is that it involves protection of the confidentiality, integrity and availability of information, also commonly known as the CIA triangle (Gordon and Loeb, 2006; Grama, 2010; Gifford, 2009; Kim and Solomon, 2010).

Gordon and Loeb (2006: 121) elaborate on each of these terms, i.e. "confidentiality (protecting private information from unauthorized individuals), availability (providing timely access to information to authorized users), and integrity (protecting the accuracy, reliability, and validity of data and databases) of information". In addition, authentication i.e. ensuring that the correct individuals are using the system, and non-repudiation i.e. ensuring that a legitimate user is not able to deny having performed a task on the system, are also presented as parts of definitions of information security (e.g. Calabrese, 2004; Gordon and Loeb, 2006; Siponen and Oinas-Kukkonen, 2007).

Information security has traditionally been technically focussed and dominated by mathematical scientists and technologists, however, it not only consists of the conventional technologies such as "access control technologies, authorisation technologies, authentication technologies, etc. but also organisational policies and procedures that are constructed into a material form by organisations" (Coles-Kemp, 2009: 181). Researchers highlight the role of policy in information security and the need for a comprehensive approach that includes people, processes and technology (Bishop, 2006; Klaic and Hadjina, 2011; von Solms, 2001) and humans play an integral role in defining information security policies and their implementation (Coles-Kemp, 2009; Albrechtsen, 2007; Stanton et al, 2005). Equally, the risks humans and

incorrect behaviour can bring to information security is also emphasised (Stanton et al, 2005; Odlyzko, 2010; Besnard and Arief, 2004).

In information security, "there is a tendency to focus on the materiality of security using epistemologies related to positivist forms of knowledge" (Coles-Kemp and Hansen, 2017: 466). Further, almost all of the literature reviewed above discusses the security of 'information', primarily from a technical perspective or where the humanistic aspects are limited to awareness and compliance (e.g. Albrechtsen, 2007; Anderson, 2003; Gordon and Loeb, 2006; Klaic and Hadjina, 2011; Lebek et al, 2013). Yet, only a brief mention of protecting 'knowledge' is made by Von Solms and Von Solms (2004). This raises the question about the value and importance of protecting knowledge of individuals, in particular *tacit* knowledge, in the discipline of information security.

Drawing upon the definitions presented by other researchers, information security in this research is defined as:

Any technical or non-technical measure taken by an organisation to prevent the loss or leakage of its valuable 'knowledge' and 'information' to third parties, whether it is intentional or accidental. Furthermore, the knowledge could be in the form of tacit knowledge (unarticulated and held by employees or embedded in processes) or explicit knowledge (codified in the form of documents or held within systems).

2.2.1 Information Security Threats

Despite organisations implementing prevention measures, information security breaches are common, thus organisations need to detect and rectify the breaches as they happen (Gordon and Loeb, 2006), although even well-established organisations that have disaster response measures in place, could still suffer significantly from a security breach (Anderson, 2003). Albrechtsen (2008: 60) argues that "although information security is resource demanding, information security breaches may cost even more". It is therefore important to understand not only the information security threats for organisations but also the prevention mechanisms that are being used in the industry.

The following sections draw attention to the types of threats i.e. human, organisational and technological, and address some of the key prevention measures that organisations have adopted.

2.2.1.1 Human

Marks and Rezgui (2009) assert that most security managers focus primarily on technical facets and solutions, yet research in the information security discipline strongly suggests that non-technical aspects are equally as important as the technical in protecting an organisation's sensitive information (Siponen and Oinas-Kukkonen, 2007; Dhillon and Torkzadeh, 2006). Siponen and Oinas-Kukkonen (2007) also argue that in many studies, due to their quantitative nature, there tends to be a lack of emphasis drawn to the non-technical aspects of information security, such as, the role of human behaviour. Crossler et al (2013) also draw the same conclusion - a predominant weakness in information security is the individual human user with the organisation, yet existing research on information security has predominantly focused on technical issues.

"Only amateurs attack machines; professionals target people" (Schneier, 2000).

Often in information security, humans are seen as the weakest link against internal and external threats (Spears and Barki, 2010; Siponen, 2000), and the vast majority of breaches of security are caused by existing internal employees (Crossler et al, 2013; Dhillon and Backhouse, 2000). This has been the case despite the significant developments in security technologies, policies and procedures (Crossler et al, 2013; Hu et al, 2012). Yet, the majority of the research carried out to prevent information security breaches is technical and concentrates on encryption and access control (Coles-Kemp 2009; Gordon and Loeb, 2006).

Not enough attention has been given to information security awareness amongst individuals and its incorporation into their behaviour in the workplace. This awareness is crucial as studies suggest that to address the information security management issues and strategies and in order to protect an organisation's information assets, human input is essential (e.g. Vroom and Von Solms, 2004; Albrechtsen, 2007; Bulgurcu et al, 2010).

Dhillon and Backhouse (2000) make the claim that an employee's integrity in their role does not always remain and once they have been employed in the organisation, the organisation needs to consider ways of maintaining their integrity. Further, it is also argued that most security breaches are caused by existing employees which could be due to pressures on individuals, personal problems such as marital, financial or medical issues, or perhaps "office romances are common backdrops for internal computer frauds" (Dhillon and Backhouse, 2000: 127). Similarly, Shropshire (2009: 296) carried out a study and found congruence to this argument where it was found that a "significant relationship exists between financial hardship, relationship strains, and the theft and sale of proprietary data by insiders; and recent firings, substance abuse, and relationship strains are related to information system sabotage". Contrarily, according to Cappelli et al (2006), the security breaches caused by humans in many cases are not spurious or with any malicious intent, but rather unintentional, accidental or out of the involved party's control.

Stajano and Wilson (2011: 70) argue that, although humans are recognised as the weakest point in information security, the responsibility does not fall entirely on their shoulders as attacks are only possible because "security engineers only thought about their way of protecting the system, not about how real users would react to maliciously crafted stimuli". Further, Coles-Kemp and Hansen (2017: 464) suggest the need for a sociotechnical approach to information security that "must be modelled to acknowledge, at least, the connection between an individual's security needs and the protection of assets".

2.2.1.2 Organisational

According to Al-Omari et al (2012), information security policy compliance is currently one of the biggest challenges and concerns for organisations. Compliance by employees is critical to making information security programs successful, but it is also argued that humans are the weakest link in the security domain, whilst they are also assets that need to be managed effectively by organisations (Al-Omari et al, 2012). Further, an employee's attitude towards compliance of security policies may be determined by possible consequences that they may experience. For example, the time and effort required if they comply or the punishment if they do not comply (Bulgurcu et al, 2010).

2.2.1.3 Technological

With the aim to become more effective, efficient and responsive, organisations have given great importance to the use of networks and IT based information and communication systems. However, the use of such systems has resulted in an increase in information security abuse (Dhillon and Backhouse, 2000). Furthermore, the increase in the use of computers and the Internet has also led to an increase in the importance of information security (Siponen and Oinas-Kukkonen, 2007). Stajano and Wilson (2011: 70) argue that "systems are often vulnerable to attack despite being protected by elaborate technical safeguards". Modern organisations require collaborative working and sharing of information between different departments, sites, clients and third parties, where such collaboration has meant that more organisations are increasingly connecting to the Internet. Yet, Herley (2009: 133) argues that, Internet related security attacks are immense and increasing as "computers are constantly targeted by viruses, worms, port scanning software, spyware, adware, malware, keyloggers, rootkits, and zombie and botnet applications". In a more recent study, Skopik et al (2016: 154) argue that the Internet threat landscape is fundamentally changing where there is a major shift from amateur attacks to highly organised, targeted and sophisticated cyber-crime that bypass common security measures, where the intensions behind such attacks are commercial.

Shropshire (2009: 297) asserts that "hackers, bots, viruses, and worms are capable of severely crippling or disabling information technologies and systems". However, this is only possible once they have gained access to the organisation's internal resources. One of the channels used to gain this access into organisations' internal resources is the use of personal Internet-enabled devices such as mobile phones and tablets. Many employees use these devices to access organisational systems, emails and data as well as their personal information and programs under the 'Bring Your Own Device' trends that many organisations allow.

*2.2.2 Information Security Meas*ures

Posthumus and von Solms (2004) make the argument that the presence of information in organisations does not only expose it to technological risks but also to people and processes that come into contact with it. Furthermore, according to Smith (2013: 20), "IT systems will never be impervious to attack – recommendations to improve seem endless. Combating a persistent actor who would like something you've got is a very hard challenge. The only solution is many solutions – a truly layered approach to security at every level – no single technical solution can help you win". Yet on the other hand, de Oliveira Albuquerque et al (2014) argue that despite heavy investments in the information security, the problem remains that it may still be insufficient to protect against security risks and breaches. It is also claimed that information security is not well understood by organisations, where the security approaches are not designed tailored to the problem itself or take into account all the necessary facets (de Oliveira Albuquerque et al, 2014).

Referring to it as 'a divided field of study', Coles-Kemp and Hansen (2017: 466) highlight the separation in information security "between the human security needs of the actors and the data security needs of the infrastructure" identified commonly in studies. The focus of information security in academic research and in practice has primarily on information technology systems, their infrastructure and protecting "positivist forms of knowledge" (Coles-Kemp and Hansen, 2017: 466) including data and information. Furthermore, Ahmad et al (2014) also argue that traditionally in information security, the focus of measures has been on protecting 'information' or 'data', and consequently, the concept of 'knowledge' has been overlooked. Thus, although information security practices are considered to be aligned with organisational goals, they typically are not designed with the aim to maintain the organisation's competitive advantage and prevent knowledge leakage (Ahmad et al, 2014).

The following sections discuss the imperative measures that organisations take to prevent theft or accidental loss of its critical business information. This includes human, organisational and technological level measures.

2.2.2.1 Human

Furnell and Thomson (2009) argue that in information security, humans are often perceived as an obstacle instead of an asset. Further, they are also of the opinion that one of the key goals of information security should be about "establishing the correct mind-set, and ensuring that people are working for (or at least with) security rather than against it" (Furnell and Thomson, 2009: 5). To inaugurate this mind-set and begin to improve individuals' information security behaviour, it is vital to create awareness and provide education of the importance and purpose of information security. Siponen (2001: 24) describes the concept of information security awareness as the process that makes humans "aware of security objectives (and further committed to them)". Furthermore, Siponen (2001) also argues that information security awareness should form an integral part of the general knowledge of individuals where anyone who sees information as an important asset, should also be aware of the potential threats associated with that information.

Not realising the fundamental importance of information security awareness between humans is described as one of the ten most 'deadly sins' of information security management by Von Solms and Von Solms (2004). In addition, Von Solms and Von Solms (2004) stress that awareness programs will make humans aware of the risks of the organisation's IT infrastructure, the potential destruction they can cause, the organisation's policies, procedures and standards, as well as the precautions that can be taken to prevent security threats.

The pace at which organisations move forward, in particular with implementing new technologies and working in collaboration with third parties and customers, make it vital for them to educate employees continually and consistently and provide awareness of the existing and potential security threats. Additionally, Coles-Kemp (2009) argues that awareness and education should be designed to respond to the cultural variations within organisations to avoid the difficult and expensive gaps from emerging between the security policies and security practices.

2.2.2.2 Organisational

The challenge for organisations is creating awareness of the policies and ensuring that these policies are followed by all employees. Al-Omari et al (2012) argue that compliance with security policies is influenced by quality of information, facilitating conditions and habits of employees. On the other hand, according to Knapp et al (2006) it is the support from top management without which the level of enforcement of security policies will diminish.

In relation to this, Al-Omari et al (2012) argue that security policies need to be designed to be effective, and this can only be achieved if users' security awareness is enhanced to comply with the policies. Thus, the role of humans in putting security policies into practice is an important element.

2.2.2.3 Technological

In academia and in practice, the focus of information security has been on technological systems and their infrastructure to protect data and information (Coles-Kemp and Hansen, 2017). Similarly, according to various researchers, a majority of the research in preventing information security breaches has also been on technically focused solutions (Gordon and Loeb, 2006; Coles-Kemp, 2009; Crossler et al, 2013; Soomro et al, 2016). Furthermore, Albrechtsen (2007: 277) argues that technological information security solutions impact and frame the users' behaviour when using information technology systems and act as a "foolproof security mechanism" when they perform an action. However, the "design of security technologies focuses on the protection of data and the usability requirements for that technology. Rarely does the security technology design process address the human security needs of the individual" (Coles-Kemp and Hansen, 2017: 464).

When looking at technical information security protection measures, it is important to do this in the context of the attributes which commonly define information security i.e. confidentiality, integrity and availability. Moreover, Siponen and Oinas-Kukkonen (2007) claim that the use of anti-virus software aims to guarantee that the requirements of confidentiality, integrity and availability are satisfied by a way of ensuring that no malicious access takes place. However, Smith (2013: 20) argues that "many organisations feel protected through simple measures such as antivirus software – which is necessary, but it's just the beginning and certainly not sufficient as part of a layered security strategy".

Organisations need to develop improved measuring mechanisms for technology related information security breaches but, more importantly, they need to develop an information security strategy first and then invest in security measures to protect their valuable information assets (Jones et al, 2009). Jones et al (2009) also stress that these measures must include investment in not only physical IT security e.g. firewalls, anti-virus programs, but also training documentation for employees on the organisation's policies and practices. Thus, the desired level of protection an organisation requires

determines the types of information security measures it implements and the amount of money, time and resources spent on these.

Ahmad et al (2014) claim that although information security practices are intended to be aligned with organisational goals, they are typically not wide-spanning and designed with competitive advantage in mind. In addition, Ahmad et al (2014) stress that traditionally in information security, the focus of measures has been on protecting 'information' or 'data', and the concept of 'knowledge' has been overlooked. On the other hand, Coles-Kemp and Hansen (2017: 466) draw attention to the gap in information security between human security needs of individuals and the data security needs of the infrastructure. Soomro et al (2016) synthesise existing information security literature and also stress the need for a more holistic approach for information security management to address such gaps. However, the practice of information security and its associated issues are starting to be recognised in recent years as wide-spanning and being considered in a wider management context (e.g. Phillips, 2013; Siponen et al, 2014; Soomro et al, 2016). Therefore, information security in the current research was recognised as a multi-layered concept that can affect the organisation in various ways which will be discussed in the Analysis and Discussion chapters.

3 Conflict between knowledge Sharing and Information Security Design

3.1 Intersection of Knowledge Sharing and Information Security

In section 2.1 of this paper, it was established that the practice of knowledge sharing is vital in order for organisations to gain advantage from their most valuable asset – their knowledge . As knowledge is a source of competitive advantage for organisations, effective knowledge sharing is critical as it benefits the organisation by creating new knowledge and enables individuals access to knowledge to support their daily activities (Raab et al, 2014; Alavi and Leidner, 1999). Knowledge sharing underpins various organisational activities and is not only encouraged, but special initiatives are often implemented to facilitate it amongst employees and partners. Through the literature review on knowledge sharing, it has also been established that research in this discipline has primarily focused on exploiting and sharing existing knowledge, and consequently the protection of knowledge has not received the necessary level of attention.

On the other hand, section 2.2 discussed how and why organisations implement information security measures to prevent and manage the loss of their valuable information and knowledge. This practice, directly or indirectly, affects the day-to-day activities of all employees in the workplace, and may also affect other partners and customers that the employees interact and engage with. However, much of the literature on information security has focused on technical aspects of information security such as technologies, access controls and policies (Coles-Kemp, 2009) – despite the integral role of constructive human awareness and behaviour in making information security practices successful being acknowledged by various researchers (e.g. Coles-Kemp, 2009; Albrechtsen, 2007; Bishop, 2006; Stanton et al, 2005; Besnard and Arief, 2004).

When the two disciplines, knowledge sharing and information security, are reviewed holistically and amalgamated, an overlapping area emerges where an inherent conflict of interest is evident. This conflict has been recognised and addressed by some researchers. For example, Figure 2, was developed by Desouza (2006) to draw attention to a research gap that he calls, 'Knowledge Security', which he claimed exists between the research areas knowledge management and information security (Desouza, 2006; Desouza and Awazu, 2004). Desouza (2006: 2) describes knowledge security as "a research space that is in dire need of attention" and emphasises the key role knowledge plays in organisations and argues that, knowledge based resources are the drivers behind other resources, consume significant amount of resources to develop and are difficult to substitute, thus, organisations need to apply significant efforts to prevent the misappropriation and sabotage of its valuable knowledge - in order to retain its value.

Similarly, Ryan (2006: 45) also addresses this conflict and argues that it is caused by the "intersection of the nature of innovation and the rewards of innovation"; innovation requires novel ideas and concepts to be imagined and shared, but on the other hand, there are needs to protect the intellectual capital that is developed from that innovation. Moreover, it is the view of Ryan (2006) that organisations typically implement information security tools and technologies by determining which information assets need protecting in terms of confidentiality, integrity and availability. However, in the context of knowledge management, different questions need to be asked when designing protection architectures, particularly with innovation and the return on investment from information sharing in mind. For example, "It may be true in some enterprises that allowing a certain amount of intellectual capital leakage could return a larger amount of innovation than keeping a very tight lid on information assets" (Ryan, 2006: 46).

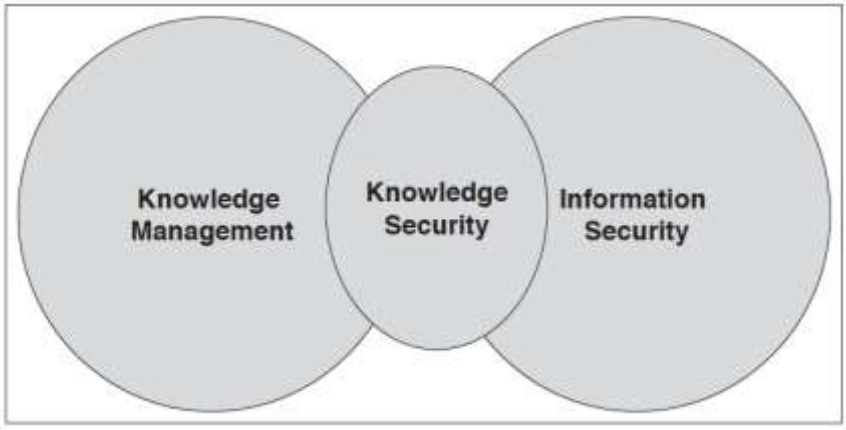

Fig.2: Knowledge security (Desouza, 2006: 2)

In a more recent study, Ahmad et al (2014: 29) argue that increasing knowledge sharing naturally increases the risk of knowledge leakage, i.e. "the need to reconcile preserving confidentiality on the one hand and increasing the sharing of knowledge on the other is a key dilemma for organizations". Pawlowski et al (2014: 83) argue that the "challenge of finding a balance between knowledge sharing and knowledge protection has been exacerbated by recent developments", particularly social technologies and social working styles where the lines between work and leisure become blurred e.g. using personal devices to access organisation's knowledge, or employees working off-site. Such social knowledge environments create challenges for compliance with legal parameters, yet a systematic knowledge protection strategy that is tailored to such environments and considers the role of social technologies in knowledge-intensive environments is often missing in organisations (Pawlowski et al, 2014).

Manhart and Thalmann (2015) conducted a literature review to understand the present state of research on knowledge protection in KM research. It is argued that the fear of security breaches and knowledge theft have led to organisations becoming security-conscious and investing in information security measures, however, paradoxically, whilst the value of knowledge assets and the importance of protecting them is widely recognised, knowledge managers do not pay sufficient attention to security issues. It is highlighted that a key barrier to knowledge protection measures in KM, is ironically, knowledge protection often being considered as a barrier to knowledge sharing, or that knowledge protection is considered as a separate part, falling into the intellectual property domain (Manhart and Thalmann, 2015). The neglect of knowledge protection can hinder exploitation of innovations, and knowledge leakage can result in loss or reputational damage, thus, "finding a balance between protecting and sharing knowledge is crucial to solving the boundary paradox" (Manhart and Thalmann, 2015: 191).

Ilvonen et al (2016) carried out an empirical study into the KM practices in various Finnish organisations, particularly focusing on their activities that promote 'knowledge sharing' and 'knowledge security' as the researchers assert that there is a need to find balance between the two practices. Moreover, it is also claimed that 'knowledge sharing' and 'knowledge security' may be seen as the 'flip sides of the same coin', both practices are intertwined which can create complex and sometimes controversial scenarios, and thus need to be managed effectively by organisations (Ilvonen et al, 2016). Ilvonen et al (2016: 4021) describe this conflict between knowledge sharing and knowledge protection as "contradictory views on knowledge" which need to be balanced.

3.2 Research Gap

By reviewing the literature on knowledge sharing and information security, and more importantly, by exploring the relationship between the two practices, an inherent conflict has been identified (e.g. Desouza, 2006; Shedden et al, 2011; Ahmad et al, 2014; Manhart and Thalmann, 2015; Ilvonen et al, 2016). Further, knowledge management has focused on facilitation of knowledge sharing and overlooked knowledge protection, whereas information security has focused primarily on technical aspects and protecting information and explicit knowledge, and subsequently neglected the development of more holistic approaches to also include knowledge protection (Manhart and Thalmann, 2015). Although, some researchers have highlighted concerns regarding the conflict and aimed to explore the area of knowledge protection (e.g. Ilvonen et al, 2016; Manhart and Thalmann, 2015; Ahmad et al, 2014; Vayrynen et al, 2013; De Faria and Sofka, 2010; Desouza, 2006; Ryan, 2006; Holsapple and Jones, 2005; Desouza and Awazu, 2004; Gold et al, 2001), the level of overall research on this topic in knowledge sharing literature, or in the wider discipline of knowledge management, is sparse.

The need for more empirical research on knowledge protection has been identified (Ilvonen et al, 2016; Manhart and Thalmann, 2015; Shedden et al, 2011; Desouza, 2006), to ensure that the valuable knowledge assets of an organisation are adequately protected as part of the broader KM strategy. Existing research mainly points towards the need for organisations to develop informed knowledge protection strategies, from a KM perspective and in the interest of protecting valuable knowledge from leakage or loss. For example, it is argued by Ahmad et al (2014) that researchers who have attempted to address the importance of knowledge protection in the past, have failed to provide appropriate guidance for organisations about the types of mechanisms required, as well as strategic and operational guidelines for protecting their sensitive knowledge. Pawlowski et al (2014) suggest that a tailored, systematic knowledge protection strategy that considers the role of social technologies in knowledge-intensive environments is required by organisations.

Similarly, according to Manhart and Thalmann (2015) a successful approach to knowledge protection would be thorough planning of systematic protection of explicit and tacit knowledge and by finding a balance between knowledge sharing and protecting. Manhart and Thalmann's (2015) view is that knowledge protection strategy should always be linked to the organisation information security strategy, as both form a vital component of risk management, and the researchers suggest that further research into how to adapt proven information security measures to knowledge protection could be of value. Ilvonen et al (2016) also identified an important issue related to 'knowledge security' awareness in organisations, where it was suggested that uncertainty about the practice amongst employees led to the assumption that protecting knowledge was merely a technological issue rather than a broader concept. This highlighted an important area about employee awareness and it was concluded that organisations need an adequately articulated KM strategy, as well as a strategy to protect knowledge (Ilvonen et al, 2016).

Reviewing the existing literature allows to understand the progress and position of research on the conflict between knowledge sharing and information security practices. However, it can also be concluded the majority of research around knowledge protection is driven by the aim to generate improved security of knowledge, and is primarily considered to be a sub-domain of KM. Contrarily to Manhart and Thalmann (2015) and Ilvonen et al (2016) who categorise knowledge protection as separate to information security, in this paper, knowledge protection is not treated as an entirely separate concept but rather considered as a part of the broader area of information security that impacts knowledge management practices, particularly knowledge sharing. Moreover, in this research, information security is considered as a broad concept, inclusive of any measures that aim to protect data, information and knowledge.

By conducting the literature review on knowledge sharing and information security, we establish certain assumptions about the concepts of knowledge sharing and information security, which elicit and clarify the following research gap:

I. Knowledge sharing and information security are in most cases entirely separate initiatives in organisations; knowledge sharing is perceived as a 'soft', human-oriented approach, whereas information security focuses mainly on technical facets.
II. Knowledge protection has not received a great deal of attention in the discipline of KM, however, the role that information security plays in how it directly impacts and overlaps KM is an underdeveloped area to an even greater extent.
III. The conflict between knowledge 'sharing' and 'security' is mainly categorised as a knowledge management issue, however, the issue arises in the intersection or overlapping areas of knowledge sharing and information security, thus a broader perspective is required to better understand this issue and to begin to create more harmony between the two practices.
IV. Previous research on knowledge protection and the conflict between knowledge sharing and security has been primarily guided by the aim to improve protection of knowledge and has typically been grounded in the KM domain; there is a need for empirical research that takes a balanced approach to exploring the practices of knowledge sharing and information security, and their middle-ground.
V. A majority of the previous research on knowledge protection, or the conflict between knowledge sharing and security has been at an abstract level and conceptually-orientated, with a lack of empirical validation.
VI. Previous research on knowledge protection, or the conflict between knowledge sharing and security, has typically taken an organisational or knowledge perspective, thus there is a need to explore the issue holistically also taking into account the employee perspective.
VII. The lack of knowledge protection theories, frameworks, strategies and guidance for organisations have been highlighted by previous literature, where the main reasons attributed to this are the lack of empirical research and the challenging nature of the conflict between knowledge sharing and security.
VIII. Information security has, for the most part, overlooked the protection of tacit knowledge and the role of humanistic or social aspects such as human awareness and behaviour, which needs further research.

4 Conclusions

To conclude, the aim of this paper was to explore the paradoxical and concurrent nature of knowledge sharing and information security and address an important yet predominantly overlooked research gap in the middle-ground between the disciplines of knowledge management and information security. This paper is the first to explore the conflict by amalgamating the two disciplines, bridging the middle-ground and understanding their relationship by reviewing and synthesizing the relevant literature, and subsequently identifying and presenting the research gap more holistically and cohesively than prior literature (see Figure 3).

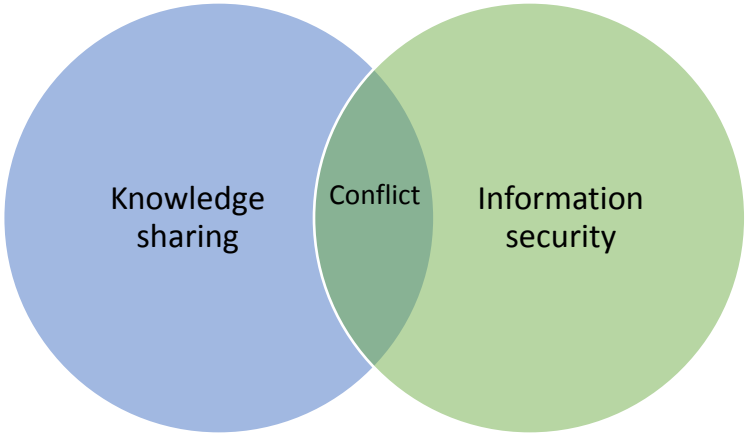

Fig. 3: Conflict between knowledge sharing and information security**.**

The existing KM literature highlighted a lack of knowledge protection theories, frameworks, strategies and guidance for organisations, due to the lack of empirical research and the challenging nature of the conflict between knowledge sharing and security. In information security literature, the protection of tacit knowledge and the role of humanistic or 'softer' aspects such as human awareness and behaviour, are often overlooked.

Prior literature on knowledge protection and the conflicting nature of knowledge sharing and information security is limited and largely of an abstract nature. Moreover, this research responds to the call expressed by various researchers for further research on knowledge protection and the conflict (e.g. Ilvonen et al, 2016; Manhart and Thalmann, 2015; Shedden et al, 2011; Desouza, 2006) and informs the existing theory. This paper contributes to developing a deeper understanding of the opposing goals and interconnectedness of knowledge sharing and information security.

Eisenhardt (1989) argues that an essential feature of theory building is comparison of the emergent concepts or theory from the data with existing literature. During this comparison, "cases which confirm emergent relationships enhance confidence in the validity of the relationships. Cases which disconfirm the relationships often can provide an opportunity to refine and extend the theory" (Eisenhardt, 1989: 542). The findings of the current research have generated both cases and thus extend previous theory, creating a solid foundation for further research, particularly empirical research, into the impact of the conflict between knowledge sharing and information security practices, which needs attention from information security and knowledge management researchers.

The conflict between knowledge 'sharing' and 'security' has mainly been categorised as a KM issue in previous literature and has been largely biased as it is guided by the aim to improve protection of knowledge, however, we argue that the issue arises in the intersection of the two practices. So, both practices need to be evaluated when researchers explore the occurrences of such conflicts and try to create a balance between them. Furthermore, unlike previous literature that also perceives 'knowledge protection' to be in the KM domain and separated from the concept of information security, based on the review of literature in this paper, we make a strong case for a change in this perception. For example, having one set of efforts for protecting knowledge from a KM perspective, and on the one hand, having separate efforts for protecting information i.e. information security – which also innately includes 'knowledge' - is an inefficient and ineffective approach that can duplicate efforts and cause confusion. Moreover, one reason for the lack of balance between knowledge sharing and information security could be the way the two practices are typically perceived to be disconnected and managed separately in organisations. This makes the subsequently arising conflicts between them difficult to identify, and requires

two separate sets of efforts for resolving the same conflict, which is a waste and duplication of organisational resources. Hence, a holistic and strategic approach to 'knowledge and information management' is proposed as a result of this research, that encapsulates the management, sharing and protection of the organisational knowledge and information to help achieve organisational efficiency and create a harmonious relationship between knowledge sharing and security.

References

[1] Morgan, J. (2014). A simple explanation of 'The Internet Of Things'. Forbs, May 13. Retrieved from: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/

[2] Scuotto, V., Ferraris, A. and Bresciani, S., 2016. Internet of Things: Applications and challenges in smart cities: a case study of IBM smart city projects. Business Process Management Journal., **22(2),** 357-367(2016).

[3] Santoro, G., et al., The Internet of Things: Building a knowledge management system for open innovation and knowledge management capacity, Technol. Forecast. Soc. Change., (2017).

[4] Attaran, M., 2017. The internet of things: Limitless opportunities for business and society. Journal of Strategic Innovation and Sustainability., **12(1),** 10-29(2017).

[5] Scuotto, V., Ferraris, A., Bresciani, S., 2016. Internet of Things: Applications and challenges in smart cities: a case study of IBM smart city projects. Bus. Process. Manag. J., **22(2)**, 357–367(2016).