
Securing intellectual assets: integrating the knowledge and innovation dimensions

Kevin C. Desouza

The Information School, University of Washington,
Mary Gates Hall, Suite 330D, UW Box 352840,
Seattle, WA 98195-2840, USA
E-mail: kev.desouza@gmail.com

Abstract: The concept of intellectual asset security has received widespread attention in recent times. Much of this attention can be attributed to the fact that knowledge assets can be used to secure competitive advantages for organisations. Moreover, one might assert that in today's knowledge-based economies and markets, it is these assets that truly differentiate organisations and are the only true source of sustainable competitive advantages. In order to have a robust program for managing intellectual assets, an organisation must account for its knowledge management and innovation processes. In this paper, drawing on

- 1 a semiotic-based model for knowledge management (Desouza, 2006)
- 2 an organisational process of innovation (Desouza et al., 2006),

the author describes an integrated process framework for the management of intellectual assets. The framework is then used to describe salient security management challenges faced when managing intellectual assets. Executives involved in security management programs in 23 organisations were interviewed to elicit key security management challenges faced by organisations when addressing intellectual assets.

Keywords: intellectual assets; innovation; information security; semiotics; security policy; technology policy; technology security.

Reference to this paper should be made as follows: Desouza, K.C. (xxxx) 'Securing intellectual assets: integrating the knowledge and innovation dimensions', *Int. J. Technology Management*, Vol. X, No. Y, pp.000–000.

Biographical notes: Kevin C. Desouza is on the faculty of the Information School at the University of Washington. He is also an Adjunct Assistant Professor in Electrical Engineering at the College of Engineering. He currently serves as the Director of the Institute for Innovation in Information Management (I3M) and is an Affiliate Faculty Member of the Center for American Politics and Public Policy, both housed at the University of Washington. His most recent book is *Managing Knowledge Security* (Kogan Page, 2007). In addition, he has published over 100 articles in prestigious practitioner and academic journals. He has received over \$1.2 million of research funding from both private and government organisations. He is a Fellow of the Royal Society of Arts.

1 Introduction

The concept of intellectual security continues to garner widespread attention from both researchers (van Wijk, 2002; Desouza, 2007; Lebson, 2007) and practitioners (see www.csoonline.com). Given today's knowledge-based competition in the marketplace and in society-at-large, this interest is justified and critical (Grant, 1996; Zander and Kogut, 1995; von Krogh et al., 2000; Nonaka and Takeuchi, 1995). The knowledge-based theory of the firm (Grant, 1996) argues that it is an organisation's knowledge resources and ability to mobilise these resources towards productive use that leads to sustainable competitive advantages. Consider the case of pharmaceutical firms. Many of these firms spend years and millions of dollars investing in research and development to discover new drugs. These expenses will only pay off for the firm once a drug is discovered, approved for commercial purposes and sales are generated. Securing knowledge-based assets is vital during the discovery and commercialisation process; the pharmaceutical firm has much to lose if information regarding its experimentation processes, the recipe of the drug and other product development details are leaked or sabotaged. Ultimately, this may cost the firm in terms of its ability to recoup its costs and earn profits.

While there is no questioning the criticality of security management to protect knowledge-based assets of the firm, there is confusion in practice as to how to manage these programs. As noted by one interviewee:

"Information or intellectual security is one of those bastard terms... to some people information security is all about securing information technology... they seldom consider the fact that most information is never transmitted through technology but through people-based interactions.... What information do you want to secure... is it the information that is in our researcher's heads or the information on how to fix the broken copier... the term information security does not really mean much, it is generic and undefined... I need something more precise... Are you talking about the security of sources of information... we do secure our databases and have legal instruments such as NDAs (non-disclosure agreements) for our employees and contractors. What about the way in which we apply information or transfer information is that part of information security? Most would consider these as part of information security only if you think in terms of electronic movement of information (e.g., through e-mails)... but what about John who goes and talks about (sensitive) information to Kelly, I have no control or cannot monitor this, but this can clearly pose a security breach... I rather (address) how we secure various items or people not about the elusive concept of information security... sorry..." – Chief Security Officer

The interviewee makes two critical points that need to be carefully considered. First, the terms information security and intellectual security are usually equated with protecting information technologies (Bertino et al., 2006; Lee et al., 2005; Memon and Daniels, 2007). This thinking is limited as many of the intellectual assets in organisations interact with non-technical artefacts. Hence, while there is an abundance of literature in the computer sciences that addresses issues such as encryption (Dobbertin et al., 2005), digital rights management (Becker et al., 2003) and other technical security apparatuses (Lee et al., 2005), these are not sufficient in order to build a holistic security program. There is a need to carefully consider both the technical and human dimensions when devising a security management framework for intellectual assets in organisations. Second, there are a limited number of frameworks to think through the management of security for information and/or knowledge in organisations (Desouza and Vanapalli,

2005; Desouza, 2007). Consider another comment by a Chief Security Officer of a biotechnology firm:

“If we are to secure intellectual assets, we must first think about innovation... innovation thrives in open spaces not in closed ones... enabling is key rather than restricting... so how can you secure such a fluid and chaotic process... wouldn't you end up killing the process... innovation is key to the development of intellectual assets... as you know, most innovators rarely abide by rules and regulations as they need to be 'free thinkers' and take 'radical approaches'... so security is a big challenge in our environment... we cannot secure at the cost of crippling innovation...”

An organisation's innovation processes are critical to the generation of intellectual assets. Innovation allows an organisation to use its knowledge-based assets in a creative manner so as to invent products and services of commercial value. As noted above, while security around the innovation process is critical, it must be balanced against the risk of unduly hampering innovation. Hence, in any discussion of security of intellectual assets it is vital to consider the innovation process. After all, if security comprises an organisation's ability to innovate, an organisation may have robust security measures with nothing to secure.

This paper puts forth a framework for the management of intellectual assets. The framework draws on:

- 1 a semiotic-based model for knowledge management (Desouza, 2006)
- 2 an organisational process of innovation (Desouza et al., 2006).

A key contribution of the framework is to account for both the knowledge management and innovation dimensions of managing intellectual assets. To the best of the author's knowledge, this is the first attempt to integrate the processes of knowledge management and innovation in a comprehensive framework. The framework is then used to describe salient security management challenges faced when managing intellectual assets. Executives involved in security management programs in 23 organisations were interviewed to elicit key security management challenges faced by organisations when addressing intellectual assets.

The paper is organised as follows: in the next section, the author describe the theoretical background for the study, including the knowledge management model (Desouza, 2006) and innovation process (Desouza et al., 2006). Both of these models were validated in previous research projects and will be described here in brief. Next, an intellectual asset management framework that integrates these two models will be presented. The research methodology is presented next. This is followed by enumeration of the key challenges faced by executives when securing intellectual assets. The paper concludes with a discussion of the implications of the intellectual asset management framework and security challenges, and areas for future research.

2 Theoretical background

The knowledge-based theory of the firm argues that an organisation's competitive advantages can be attributed to the dynamic processes which integrate the knowledge-based resources possessed within a firm and those that can be accessed by the firm (e.g., through strategic alliances) in a manner that is superior to its competitors

(Grant, 1996; Kogut and Zander, 1992; Teece et al., 1997; Zollo and Winter, 2002; Nonaka, 1994). For the purposes of this paper, knowledge-based assets are defined as the collection of both knowledge-based 'resources' and knowledge-based 'processes' that are used to mobilise and leverage an organisation's resources.

Knowledge-based assets, both resources and processes, have interesting properties – they encapsulate experiences and path dependencies (Rosenberg, 1994; Garud and Karnøe, 2001). These assets take time, energy, and resources to develop, and they are seldom purchased off-the-shelf. The time it takes for organisations to craft and develop these assets means that losing these assets leaves a void that cannot be easily filled. Knowledge-based assets are built over time; that is, they have history. Once again, consider pharmaceutical companies developing the next drug through extensive research and experimentation. The cost of these exercises is not cheap, both in terms of real cost (dollars spent) and opportunity cost (hours spent). Each successive experiment is viewed as a learning episode and future experiments build on the lessons learned. Now, imagine if the results of some experiments were misplaced or leaked due to sloppy behaviour on the part of the employees. Not only would this breach diminish the value of these specific experiments, but also with some level of creativity, it would be easy to extrapolate other operations within the organisation. Exposure of path dependencies is a critical problem, as this may negate most efforts that went into charting these courses and will call for the organisation to reconsider its plans, which is not easy to do.

The value of an organisation is intimately tied to the ability to manage knowledge assets and innovate. The knowledge management process helps a firm leverage its explicit and tacit knowledge bases, while innovation is the process by which a firm encapsulates its knowledge into tangible products and/services of commercial value. Managing knowledge is most commonly associated with the enabling of the codification, storage, retrieval and application of explicit knowledge and the sharing of tacit knowledge (Nonaka, 1994; Davenport and Prusak, 1998; Davenport et al., 2003). Unless a firm has an adequate grasp of its knowledge management process, it will lack the ability to apply its knowledge base in an optimal manner. However, simply managing knowledge is not sufficient. Knowledge management must be coupled with the firm's innovation abilities. Through the process of innovation, a firm refines its knowledge base (Nonaka, 1994). Innovation requires a firm to interact with external entities (e.g., customers, business partners, etc.) and promote interactions among its internal entities (e.g., individuals, teams, groups, etc.). It is in these interactions where the prominence of security comes to the forefront. Interactions on knowledge assets require the exchange of information and/or knowledge of a sensitive nature with entities that may be outside the control of the organisation. Similarly, even if one were to consider the internal perspective, an organisation must allow for employees to share, exchange, manipulate and apply knowledge without extensive controls and overhead to promote the development of inventions, which hopefully might be commercialised as innovations. Hence, it is quite critical to consider the process of innovation and knowledge management processes when analysing security issues surrounding intellectual assets.

To appreciate the competitive power of intellectual assets, one must carefully consider the security dilemma when considering how to manage knowledge and foster innovation (Desouza, 2007; Desouza and Vanapalli, 2005; Hackney et al., 2005). On the one hand, knowledge and innovative capabilities possessed by an entity (e.g., individual, group, organisation, etc.) can be a source of competitive advantage. The amount of profit an entity can earn from its knowledge can be traced to its scarcity in the environment

[Larsson et al., 1998; Smith, 1910 (1776)]. All other things being equal, the greater the scarcity of the knowledge, the larger the rent one might expect to earn. As such, entities have an innate desire to keep their knowledge scarce and to protect it (Kumar and Nti, 1998). Similarly, it is quite conceivable that while knowledge on a given topic might be common in the marketplace, an entity might possess innovative capabilities to integrate and put the common knowledge to productive use at a superior rate compared to others. In this case, the entity should retain the competitive value of the process by securing it and preventing others from duplicating or sabotaging it.

On the other hand, knowledge remains a social good (Cohen and Prusak, 2001) and as noted earlier, invention and innovations require collaborations with external entities. Entities need to collaborate and share their knowledge in order to:

- 1 enrich their individual collections of knowledge
- 2 contribute towards to the attainment of collective objectives
- 3 access complementary resources that are possessed by external entities.

First, an individual's knowledge base gets refined through interactions with peers (Nonaka, 1991). Through dialogue and exchanges, individuals share their experiences, expertise and know-how and also receive these from their peers. Second, in collective settings, the attainment of objectives is dependent on how effectively and efficiently each individual shares his/her knowledge with the group (Nonaka, 1991; Nonaka and Takeuchi, 1995; Davenport and Prusak, 1998). Third, it is unlikely that any entity will be self-sufficient and possess all resources necessary to meet its objectives. In today's marketplace, the prominence of knowledge-based exchanges, especially in the context of accessing complementary resources from external parties (e.g., business partners, etc.), continues to gain prominence through mechanisms such as strategic alliances, joint ventures, etc. These arrangements necessitate the sharing of knowledge. Moreover, the ability of a firm to innovate is deeply tied to its ability to collaborate with external entities (Chesbrough, 2003; Hagel and Brown, 2005; von Hippel and von Krogh, 2003). Firms must jointly develop innovative products and services and even jointly develop their strategic capabilities. Successful collaborations for innovation require firms to share their knowledge, work with their partners to co-create products and/or services of value and build partnerships for successful commercialisation of these.

To summarise, a firm cannot afford not to assume any risk and lock down all its knowledge-based resources, as this action may prevent the firm from integrating and leveraging these for productive purpose. However, at the other extreme, the firm cannot unconsciously and carelessly allow external entities to access its knowledge-based resources, as this will lead to lose of competitive advantages. The ideal organisation must have a security management program that is cognisant of balancing the need for protecting knowledge-based assets from unauthorised entities, while enabling for its optimal sharing among authorised entities. Appreciating this reality calls for an understanding of the knowledge management and innovation processes.

3 Organisational knowledge management

Most firms follow a process whereby knowledge-based resources are constructed – the knowledge management process (Davenport and Prusak, 1998; Davenport et al., 2003).

The most popular concept involving knowledge management includes a depiction of the process whereby data and information are synthesised to create knowledge intended for decisions (Alavi and Leidner, 2001). Knowledge can be defined as a collection of justified beliefs that increase an entity's capacity for action (Nonaka, 1991; Huber, 1990; Polanyi, 1958, 1966). Synthesis of data and information pertaining to these beliefs is used for the purpose of justification. In order to manage knowledge optimally, it is necessary for an organisation to be able to control four crucial components:

- 1 acquisition of information and knowledge
- 2 the processing of information and knowledge
- 3 the creation, storage, transfer and retrieval of knowledge
- 4 the application of knowledge (Desouza, 2006; Davenport and Prusak, 1998; Nonaka, 1991; Davenport and Grover, 2001; Alavi and Leidner, 2001).

Failure to conduct activities within these components in an optimal manner could result in a knowledge management program that is wanting and incomplete. Currently, the literature on knowledge management is vast, yet still growing (Nonaka, 1991; Nonaka and Takeuchi, 1995; Davenport and Prusak, 1998; Davenport et al., 1998; Davenport and Grover, 2001). However, as noted in Desouza (2006), most organisations lack an adequate process by which to manage knowledge.

In order to examine knowledge management in organisations, we need to focus on the generative (how knowledge is produced) and dissipative (how knowledge is applied) (Ramaprasad and Rai, 1996; Ramaprasad and Ambrose, 1999; Desouza 2006; Desouza and Hensgen, 2005). The generative dimension calls for leveraging data and information to create knowledge; the dissipative aspect calls for ensuring that knowledge is used to inform actions and change the behaviour of the organisations. As asserted in Desouza (2006), the discipline of semiotics (Saussure, 1916) can be used as the basis for any concept of knowledge management, as it embraces both the generative and dissipative aspects of knowledge management. The discipline of semiotics (Saussure, 1916) seeks to investigate the nature of signs – containers of information – and the governing laws that affect them. Semiotics can be broken down into four distinct domains: morphology, syntactics, semantics and pragmatics (Saussure, 1916). Morphology is the study of the sources of signs. Syntactics is the study of the formal relations between signs, semantics is the study of the meaning of signs and pragmatics is the study of signs in relation to an interpreter's actions. Data objects are signs; they signify a measurement of something. Information is formed by connecting, synthesising and integrating data objects to form an organised assemblage – the syntactics. Information put in context helps us garner meaning (the semantics), and based on the meaning we can choose appropriate courses of action (the pragmatics).

Desouza's (2006) knowledge management model is segmented into four components: sources management, analytics management, interpretation management and action management. These components map onto the four domains of semiotics as follows: sources management (morphology), analytics management (syntactics), interpretation management (semantics) and action management (pragmatics). The components are presented in escalating order of complexity, as each determines the basis upon which the others will build on sequentially. In addition to being able to execute each component of knowledge management, it is highly advisable for the organisation to move through the

phases in a timely manner, since elements related to knowledge are perishable and subject to rapid change. Timely generation and dissipation of knowledge are critical for building the real-time enterprise (Economist 2002a, 2002b, 2002c). An organisation needs to show proficiency in all four components in order to have a successful knowledge management program.

Through an inter-disciplinary investigation of the literatures in information systems, economics, education and learning, information science, computer science, public policy and strategic management, among others, Desouza (2006) develops theoretical definitions for knowledge management and each of the four components (sources management, analytics management, interpretation management and action management). For each component, a set of critical capabilities are also outlined. These capabilities represent critical activities that an organisation must conduct in order to meet the goals of the component. Desouza (2006) took a qualitative approach to validate and refine the definition of knowledge management, the definition of each component of knowledge management and the list of critical capabilities for each component. Semi-structured interviews with over 20 executives responsible for knowledge management programs in their organisations were conducted. The organisations selected represented a wide-range of industries and sectors (product, service and knowledge), from management consulting, information technology, pharmaceutical, legal, university libraries and defence, among others. The validated definition of knowledge management is as follows:

“Knowledge management is defined as the collection of activities involved in managing the sources of information, analytics used to derive relationships from information, mechanisms for interpreting meanings from relationships and calibrating actions based on meanings, in an effective and efficient manner, to meet the challenges of the organisation. The components, sources management, analytics management, interpretation management and action management, are in escalating order of dependence as each determines the basis upon which the others will build upon sequentially. The components of knowledge management are linked with one another in a circular manner. The goals of knowledge management are to contribute to increased business value of the organisation and also to improve the process of knowledge management in the organisation.” [Desouza, (2006), p.283]

The above definition argues that knowledge management should not to be viewed as a monolithic construct (Desouza, 2006), but seen in relation to the four components. An organisation may demonstrate excellent execution of one component yet lack proficiency in others, thereby hindering a well-intentioned knowledge management process. Moreover, the definition focuses attention on the concept of business value. Knowledge management should contribute to enhancing the business value of the firm. Knowledge management enhances business value by providing a mechanism whereby to leverage its knowledge-based assets. Put another way, the firm has a mechanism by which to ensure that it uses its knowledge-based assets in an optimal manner so as to create intellectual assets. Furthermore, the definition notes that the four components of knowledge management, while self-contained, are also tightly coupled. Table 1 contains the validated definition for the four components of knowledge management and the list of critical activities. The author will now briefly describe each component [the interested reader is referred to Desouza (2006) for further information].

Table 1 Knowledge management model

<i>Concept</i>	<i>Definition</i>	<i>Capabilities</i>
Sources management	“The objective of sources management is to ensure that the organisation uses the right sources to obtain the right information, of the right quality, at the right time, at the right cost. Sources are the agents (human) and objects (physical) that possess or emit information of interest to the organisation. To do so, the organisation has to know its current sources and the characteristics of the information they provide. It has to protect the sources and retrieve information from the sources in a timely manner. It has to continuously evaluate these sources and seek new sources as its internal and external conditions change.” [Desouza, (2006), pp.283–284]	<ol style="list-style-type: none"> 1 Identifying sources 2 Evaluating source characteristics 3 Organising sources 4 Retrieving information from sources 5 Protecting sources 6 Updating the collection of sources
Analytics management	“The objective of analytics management is to ensure that the organisation uses the appropriate analytical tools to discover and validate relevant logical and empirical relationships using the information it has from various sources. To derive the relationships, the organisation has to deploy a range of heuristic, mathematical, statistical, logical and qualitative techniques. It has to continuously evaluate these techniques and seek new ones as its information base changes. The organisation has to maintain the right skill base so that analytics can be conducted in an effective and efficient manner.” [Desouza, (2006), p.284]	<ol style="list-style-type: none"> 1 Discovering relationships 2 Visualising relationships 3 Validating relationships 4 Training users 5 Reusing analytical tools 6 Devising an analytical framework 7 Managing and evaluating analytical tools
Interpretation management	“The objective of interpretation management is to ensure that the organisation correctly interprets and tests the meaning of logical and empirical relationships discovered through analytics. The relationships have to make sense in the context of the organisation and its environment. To derive the meaning of relationships, the organisation has to deploy a range of computer, individual and group based methods. It has to continuously evaluate these methods and seek new ones as its information base and relationship types change.” [Desouza, (2006), pp.284–285]	<ol style="list-style-type: none"> 1 Generating interpretations 2 Testing interpretations 3 Sharing interpretations 4 Storing interpretations 5 Evaluating and updating interpretation methods
Action management	“The objective of action management is to ensure that the organisation responds correctly based on the interpretations of the relationships discovered using the information from various sources. The actions may be physical or logical. To transform meaning into action the organisation has to draw upon its repertoire of experience encoded in its people, processes and systems. It has to continuously evaluate and modify this repertoire based on its learning from the outcomes of past actions.” [Desouza, (2006), p.285]	<ol style="list-style-type: none"> 1 Constructing actions 2 Coordinating actions 3 Executing actions 4 Reusing actions 5 Communicating actions 6 Communicating actions 7 Learning from actions

The component of 'sources management' is concerned with:

- 1 management of sources of information
- 2 the acquisition of information from sources of interest (Desouza, 2006).

This component serves as the foundation on which a sound knowledge management program can be constructed. Organisational problems can be traced to lack of attention to signals emitted by relevant sources (Mitroff, 1988). Organisations will not be able to generate and apply knowledge in a timely fashion unless information from the source is received and attended to. Lack of attention to the sources may lead an organisation to use incomplete, non-credible and non-validated information. The organisation will then succumb to the garbage-in-garbage-out (GIGO) syndrome.

The first capability that an organisation should possess is the ability to identify sources of interest from its internal and external environments. These sources represent the elements from which it will seek to gather signals in order to gauge changing conditions in the environment. Not all artefacts, physical or logical, are sources of interest to the organisation. To the contrary, one of the challenges of the organisation is to reduce the amount of noise, i.e., being able to focus its attention on sources that truly matter. The second capability, evaluating source characteristics, points attention to the need for organisations to have procedures for making assessments on a source's credibility, reliability, authenticity and value. In addition to making assessments on the source, the organisation must have the ability to screen the signals it receives from a source. For example, we may have a source that is very reliable but may provide information of limited value. Similarly, we could have a source with sporadic reliability, but the information they provide could be of high value. Hence, evaluation protocols need to be in place for both the sources and the information they provide. The third capability is one of organisation. Sources of interest may be unevenly distributed across the organisation. Individuals may have access to sources that are unknown to their peers. Similarly, access to sources may be confined to a given team or group. The ideal organisation will create a map of sources, which shows:

- 1 where sources reside within and across the organisation
- 2 how sources can be accessed and by whom
- 3 how sources are related to each other.

Fourth, the ability to retrieve to information from sources in a timely manner is critical. Moreover, choosing the appropriate method to retrieve information from a source is equally important. Applying the wrong information retrieval method for a given piece of information and/or a particular source could prove to be highly problematic and result in negative outcomes (e.g., delays in retrieval, inability to retrieve information, etc.). Fifth, the capability of updating the collection of sources is critical as organisations compete in a time-dependent and dynamic environment. It is imperative that each organisation continuously renew and update its collection of sources. New sources must be added on a regular basis and old sources must be purged. A given source may become eligible to provide new sources of information as well. The final capability, protection of sources, is one of direct saliency when considering security issues of knowledge management. Acquiring valuable sources of information is a time consuming and costly process. Time and resources are needed to scan the environment for valuable sources, evaluate sources,

in some cases even develop sources (e.g., the development of sources in the context of human intelligence operations in the government), organise them and maintain them. While not all sources may provide an organisation with information that results in 'sustainable competitive advantages', most sources being managed should provide the organisation with some value. Organisations need to be able to protect their sources in order to preserve their value. Doing so requires an organisation to understand the value proposition for a given source, the criticality of the information being provided by the source for current and future business operations and the appropriate security mechanisms might be employed for protection.

While sources management was concerned with sources and the information they provide, 'analytics management' is about processing (analysing) the information so as to identify valid relationships (i.e., trends, patterns, correlations, cause-effect, etc.). The analysis of information involves processing by both humans and machines, acting separately or in concert. From the vast volumes of information with which an organisation may come in contact, only a portion is put through analytics management. Organisations may characterise some information as un-analysable. This is because the information presented may be non-routine or economically costly to analyse (Daft and Lengel, 1986). While all organisations may have some information that falls into this category, it is always worthwhile to analyse most information from sources. Reducing all or most of the information to the un-analysable category demonstrates lethargy on part of the organisation and will result in poor execution of actions.

The first capability within analytics management is the ability to discover relationships. Due to the sheer volume, variety and rate at which an organisation is bombarded with information, it becomes impossible to manually sort through information elements at the individual level. It would be beneficial for the organisation to determine a desirable rate at which to process such information in order to discover, develop or investigate useful patterns. An organisation should be able to connect information emitted from varied sources that may reside in a wide array of organisational domains. This is necessary to understand the totality of 'the big picture'. The ideal organisation will also possess the capability to easily visualise information. Information visualisation (Tufte, 1990) has become critical given the complexity of information relationships and the inability to depict these complexities in standard textual or mathematical formats. Information relationships must be put through a process of validation. The capability to validate relationships calls for the ability to assess and evaluate information relationships. Technological sophistication and user-friendliness has had a double-edged sword effect on the management of analytics. On the positive side, technology has contributed to the ease by which routines can be developed or coded. Today, business professionals can write routines to manipulate information without the need for intervention or support from computer scientists. But such familiarity breeds its own form of problems: routines written are seldom put through the same rigor or validation and integration for which they have been developed. Since they may not be used in the manner for which they were intended, certain 'steps' are sometimes skipped in pursuit of quick results. For example, while it is relatively easy to secure software intended to do statistical analysis – e.g., SAS or SPSS – those unfamiliar with statistics can feed numbers into such programs to produce 'results' that are as imposing as they are worthless. Similarly, it is possible that incorrect routines could be used to process information. Hence, the capability of training users becomes crucial. Users must be knowledgeable on how to process information in an appropriate manner that adequately accounts for the nature of information, the source

from which the information was acquired and the prevailing business context. What is troubling is that poorly calibrated routines could make their way to organisational repositories and be subject to re-use throughout the organisation, thereby impacting the capability of reuse of analytical tools. Consider for example, that the re-use of software code has been touted by many to dramatically improve the speed, reliability, and ease by which programs are composed (Davenport and Desouza, 2003). However, the re-use of bad code can cause other sorts of problems, especially since re-used code is seldom re-tested prior to use on new problems. It would be beneficial for an organisation to maintain a repository to hold the analytical routines. The repository could then be used to promote re-use of routines among the organisational members. An ideal repository will contain validated analytical routines that are easy to customise and deploy for multiple purposes within the organisation. Organisational members should contribute their routines to the repository, so that other personnel do not engage in re-inventing routines and duplicating effort. Mechanisms that are put in place to validate routines before they make their way into the organisational repository will be decidedly beneficial and prevent poorly or incorrectly calibrated routines from being used. The ideal organisation will also have a framework that governs how analytics are conducted. This framework will promote the portability of information relationships, reports and analytical routines across internal (e.g., individuals, teams) and external entities (e.g., business partners). The framework will ensure that standards are set as to how to define the measures by which information relationships are deemed credible, reliable and valid. In addition, it will specify who is responsible for given relationships and how best to go about calibrating information relationships in an optimal manner. Finally, the capability of managing and evaluating analytical tools calls for:

- 1 ensuring integration among various analytical tools
- 2 updating, upgrading and acquiring analytical tools as necessary to meet changing conditions in the environment.

Once information is processed, the next step involves sense-making (Weick, 1995; Nonaka, 1991; Huber, 1990). The concept of 'interpretation management' is concerned with this aspect of the knowledge management process. Without shared meaning, any attempt at the organisation of distributed or disparate components becomes near impossible. Meaning helps establish context and provides a basis for the communication that is essential for an organisation. Any generated analysis needs to be interpreted using the meaning that resides within the organisation and it necessarily has to, in some manner, reflect on the existing meaning in order to modify any interpretation that reflects new realities (Weick, 1995).

Organisations must have the ability to make sense of information relationships. Doing so is a two-fold task. First, the organisation must be able to use its knowledge-base to make sense of new information relationships. Second, new relationships discovered should contribute to increasing the richness, depth and accuracy of the organisational knowledge base. Generating interpretations calls for the ability to bring knowledge workers in contact with analysed information and with each other. Unless information is made available to knowledge workers, they will have limited ability to interpret it and make sense of changing conditions in the marketplace. In addition, organisations continue to structure themselves along horizontal rather than vertical paths (Galbraith, 1994; Lawrence and Lorsch, 1967). The benefit of horizontal structures is their ability to

quickly adapt to changes and share information spatially in an effective manner; however, they call for greater effort in terms of coordination of efforts. In traditional vertical structures, communication flows in a rigid top-down fashion, while in a horizontal structure, communication flow is emergent and, therefore, needs extra care by management. The burden for the organisation is to identify the means of coordination 'a priori' and to also have flexibility for ad-hoc or emergent coordination, so as to bring the required knowledge workers in contact for sense-making activities.

The next two capabilities of testing and sharing interpretations require serious considerations. Similar to the arguments made while discussing analytics management, it is quite critical to ensure that interpretations are put through testing to ensure that we do not have the propagation of incorrect assessments. To do so, the organisation must have mechanisms to ensure that interpretations are debated, which necessitate the ability to share interpretations among knowledge workers. The sharing of interpretations is more difficult and complex than information transfer. Interpretations, unlike information, is dynamic and in a constant state of change (Nonaka, 1991; Berger and Luckmann, 1967; Desouza and Hensgen, 2005). Unlike information, interpretations (knowledge) are heavily context-dependent. Interpretations that are useful in one context may not have any value in another; moreover, knowledge may lose its value while being communicated from one context to another. It is also useful to remember that interpretations are sticky (von Hippel, 1994), i.e., it is not easy to move from one location to another, and the cost of moving knowledge increases as the distance between source and recipient increases. One of the critical reasons is the effort needed to code knowledge in a language that retains the value and meaning of the original insight. Moreover, while language helps in communicating meaning, it is only useful if organisational participants are open to listening to what is spoken. Getting the different communities of practice (CoPs) to engage in conversations and share meaning, as argued by Boland and Tenkasi (1995), involves perspective taking and perspective making. It would be greatly beneficial for each CoP to be willing to engage in joint decision-making activities with other communities, to be able to share knowledge and ideas, thereby alleviating contextual issues, and to be willing to accept knowledge from the outside. Besides lateral exchanges of meaning between CoPs, meaning must also move from the individual level to the group/team level and finally make its way to the organisational level (Nonaka, 1991; Weick, 1995; Daft and Weick, 1984). The role of the organisation becomes that of the coordinator, whose job is to integrate the work in communities to meet the corporate agenda (Kogut and Zander, 1992).

The capability of storing interpretations calls for building an organisational memory (references). An organisation will be served well if it has the ability to record experiences and use these for future interpretative exercises. Here, it is important to pay attention to the form (Daft and Wiginton, 1979; Boland and Tenkasi, 1995) in which interpretations are coded for recording purposes and how best to promote the development of organisational memories rather than simply having each individual entity store interpretations locally. An organisation will need to update meanings on a regular basis. Meanings need to be updated to reflect adaptations to the environment but, more importantly, it would be advantageous for an organisation to proactively modify behaviour to sense changes to the environment. Being reactive has its drawbacks, including the fact that it signals predictability. In the current environment, the dynamic and ever-changing nature of meaning is very significant and an organisation found to operate on old meanings will find itself at a distinct disadvantage. An organisation profits

from equipping its agents with the ability to optimally generate meaning. Employees need to keep their skills updated on a constant basis in order to be able to make sense of an ever-changing environment. Moreover, an organisation benefits from having the right influx of new knowledge sources to complement its existing knowledge base. Both the sources of interpretation (i.e., the knowledge workers) and how these workers collaborate and interact with each other to form interpretations may need to be updated on a regular basis, either because the current methods for interpretation are faring poorly or changes in the environment call for innovative methods.

The final component is 'action management'. Up to this point, the processing and input aspects of knowledge management and the need for their effective management have been outlined. However, without an appropriate output, the value of the process is diminished or nullified. The knowledge generated is used to inform organisational behaviour, improve the negatives or weaknesses of the organisation and reinforce the positives to increase the strengths of the organisation.

Interpretations (the logical) will need to be transferred into actions (the physical) (Ramaprasad and Rai, 1996) – generation of actions. For routine problems, where there are existing actions that can be re-used, the organisational memory plays a salient role. Routine problems call for exploitation of existing solutions. For novel interpretations, the organisation needs to invest time and effort to create actions, thereby calling for exploration. The organisation will gain from the ability to calibrate the new action and then transfer it to members who will enforce the action; in addition, the action will ideally make its way into the memory of the organisation. As pointed out by Langley (1995), organisations can be paralysed by over-analysis or succumb to extinction by intuition, the two extremes of how actions are calibrated. On one hand, over-analysing a problem and spending inordinate time analysing the information will prevent the organisation from acting in a timely manner to counter the problem. On the other hand, if all actions are based on hunches, feelings and guesses, mistakes are likely. The challenge for the organisation is to strike the right balance between these two extremes. Once calibrated, actions need to be executed. Execution of actions can occur either by the creators of the action or by other members of the organisation. In the latter case, mechanisms need to be in place to effectively and efficiently communicate and coordinate actions. It is important to bear in mind that the noise in communications should be minimised, so as to avoid distorted or incorrect actions from being executed. Communication is important in action management, as it was in interpretation management.

Actions can be coordinated by either structuring them in a sequential manner (i.e., one after the other), in a parallel manner (i.e., ensuring that all actions being conducting at the same time are not in conflict) or in a hierarchical-override manner (i.e., where there are superior actions or high priority actions that may dominate other others). The capability of re-using actions is critical; as it is desirable for an organisation to build a repository of actions that can be drawn on to contend with future problems – the organisational memory (Huber, 1991; Walsh and Ungson, 1991). Actions need to make their way into the memory of the organisation, in order to be recalled for addressing recurrent problems (March and Simon, 1958; March, 1991). It is a waste of time to reinvent actions to deal with similar problems. It is insufficient to only capture the action in the memory; it is necessary to also capture the context surrounding the action. Solutions to problems are context-specific. The capturing of context is essential, as it helps add explanations or rationales to actions. Instead of merely instructing an action,

providing an explanation to the action adds more credibility to the act. Moreover, the context will help link or connect related actions. Learning from actions will also be promoted through capturing context. By documenting an action, the organisation begins to store the end-results, which enables comparisons with the original expectations. In addition to capturing the objective outcomes of an action, some of the methods described for documenting the subjective outcomes of actions include conducting post-mortem analyses, debriefings and polling the stakeholders of an action. Organisation members can dissect and reconstruct the decision-making process in order to study the underlying causes of the problem, the nature of the solutions and how the two interact. Successful resolutions to problems can serve to bolster the overall work process and contribute to the knowledge base and memory of the organisation. Unless an adequate organisational memory is in place, effective learning may be difficult. In reviewing the metrics leading to an action or implementation, the organisation will benefit measurably from the ability to gauge the effectiveness of the act. Evaluation is of importance as actions are only good if they meet their intended objectives. Feedback (Argyris and Schön, 1978) may require the organisation to modify (or stop) current actions as they may not be giving the intended benefits.

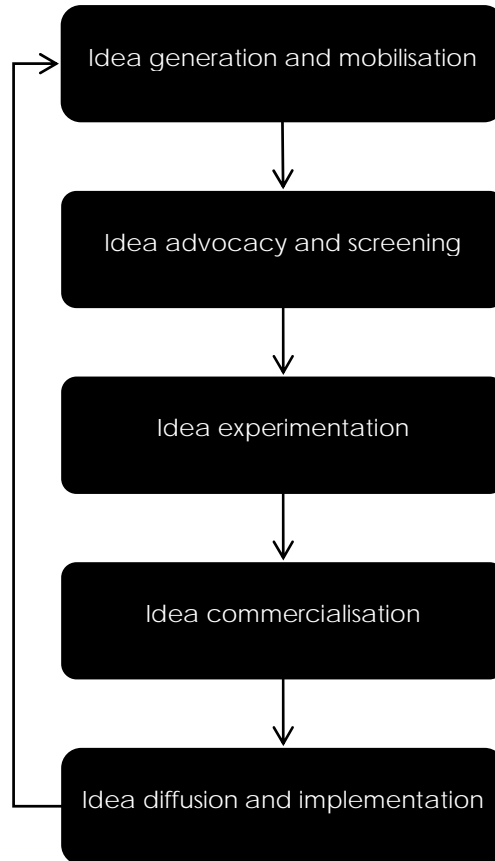
In summary, knowledge management is comprised of the components of sources management, analytics management, interpretation management and action management (Desouza, 2006). For each component, we have a list of critical capabilities that must be executed. While knowledge management is critical for the creation of intellectual assets, it is not sufficient. Fostering innovation within the organisation is critical for the development of intellectual assets. Innovation is necessary to arrive at novel knowledge and arrive at innovative methods to conduct each of the components of knowledge management. In the next section, we describe a process for organisational innovation.

4 Organisational innovation process

Similar to the process model used to describe knowledge management, Desouza et al. (2006) constructed and validated a process for organisational innovation. Drawing on an examination of innovation programs in over 30 global organisations, spanning a diverse set of industries, Desouza et al. (2006) describe a process for innovation and articulate how practices in each stage of the innovation process differ between robust and brittle organisations. Robust organisations are those who have shown the necessary capacity to build and manage sustainable innovation programs. Brittle organisations, in comparison, have only limited success at innovation, if any at all.

The innovation process is broken down into the pieces of:

- 1 idea generation and mobilisation
- 2 idea advocacy and screening
- 3 idea experimentation
- 4 idea commercialisation
- 5 idea implementation and diffusion (Desouza et al., 2006) (see Figure 1).

Figure 1 Organisational innovation process

It is critical for an organisation to show competency in all components of the innovation process. The author will now describe each stage of the innovation process in brief [the interested reader is referred to Desouza et al. (2006) for details].

The innovation process begins with ‘idea generation and mobilisation’. Ideas are the inputs into the innovation process. Ideas either may be generated by an entity or may be acquired from the outside. In cases where ideas are acquired from the outside, mobilisation becomes important. In today’s environment, it is necessary for an organisation to enable both internal idea generation and promote the acquisition of ideas from external sources (Chesbrough, 2003; Hagel and Brown, 2005). Most organisations realise, and appreciate, the reality that not all ideas for innovation are going to come from internal sources. Ideas from customers, business partners and even from other external sources (e.g., government, academia) can be very valuable (von Hippel and von Krogh, 2003; Chesbrough, 2003). Organisations must have a good inventory of sources from which they draw ideas. This calls for balancing between exploitation of ideas from known sources and exploring novel search spaces for new sources and ideas. A critical issue that needs to be appreciated during the mobilisation of ideas is that not all ideas will transport well. Ideas that work well within one context will not work well in others. Hence, care must be taken so as not to generalise an idea beyond its bounds. Furthermore,

care must be taken so as not to lose the idea during the translation and transfer processes as these may render the idea useless. The ideal organisation will know how to balance between internal generation of ideas and mobilisation of ideas from the external environment, while engaging in both exploration of new sources and exploitation of existing sources.

The next step is one of advocating and screening ideas. Most organisations do not have any deficiencies in the volume of ideas with which they are bombarded; the challenge of identifying the ideas that have commercial potential is more salient (Desouza et al., 2006). Advocacy and screening are, to a certain degree, opposing forces; ideas with commercial potential need to be both advocated for and put through a screening process. In many cases, the entity that developed the original idea will be a poor advocate for it, as the entity may not be able to clearly articulate the idea and may lack the necessary resources (e.g., power, budget, etc.) to get the necessary support for the idea. Many times, it is the peers and superiors of the individual who help in advocating for the idea. In order to adequately screen ideas it is critical that the organisation have the necessary protocols in place to discern the value of an idea (e.g., the cost and budgets needed), its innovation potential (for, e.g., will the idea foster radical or incremental innovation) and the time to market (e.g., near-term or long-term). Screening for ideas of an incremental nature is an easier proposition when compared to evaluating ideas that may have potential for radical innovation. The ideal organisation will need to have in place a set of analytical capabilities that it can draw on to ensure that ideas are connected with one another so as to foster collaborative innovation and to ensure that the necessary synergies are developed between the various idea creators, mobilisers, advocates and screeners. This will add to the effectiveness and efficiencies, of advocating and screening protocols. For example, situations might arise when two or more discrete ideas when considered individually are weak, but when considered in combination could signal an area of radical innovation due to their inter-disciplinary nature.

Once ideas are advocated and screened, the next step involves experimentation. In this stage, the idea is prototyped, tested, refined and enhanced. Most often, external stakeholders (e.g., customers, business partners, etc.) are called to participate in this stage and their feedback is used to improve the prototype and develop commercialisation plans (the next stage). Ideally, an organisation will have robust processes for experimentation that are both structured and defined, while allowing for emergence and flexibility (Desouza, et al., 2006; Thomke, 2003). Structured and defined processes are essential as they promote economies of scale and also allow for the sharing and collaboration during the experimentation process. However, they should not restrict or inhibit innovation in the experimentation process. An appreciation for the emergent nature in which experiments might manifest themselves is essential. The critical goal of this stage is to interpret the results of the experiments in the context of the business – i.e., can the product and/or service developed from the idea be commercialised, and, if it can be commercialised, do the expected returns compensate for the cost of commercialisation? Generating, sharing, testing, refining and storing, interpretations are important at this stage. Interpretations conducted within the realm of one experiment need to be interpreted within the context of prior experiments and those that might be conducted in the future.

The next stage helps move the product and/or services to the market. At this stage, actions need to be coordinated and integrated across the organisation in a unified manner

so as to launch the new product and related services. Commercialisation calls for coordination not only horizontally (i.e., across all departments in an organisation), but also vertically (i.e., across business partners and suppliers). In addition, chances are high that during this stage the organisation will reuse portions of its previous commercialisation efforts. This is necessary so as to focus resources on novel areas, rather than reinventing existing areas of competency.

Once commercialised, the organisation must ensure that the products and services are diffused in the marketplace. Diffusion involves getting customers to accept the new products and services, try them out, purchase them and consume them to enhance their daily lives. The organisation must learn from the implementation efforts of, and with, customers and use this feedback to improve their future innovative efforts. Evaluating the success (or failure) of the commercialisation effort is salient as the use of this feedback should trigger learning within the organisation and must be used to rectify failed processes and strengthen successful ones.

In summary, the innovation process is concerned not only with designing inventions, but also ensuring that the organisation can earn rents from the successful commercialisation of the inventions. The innovation process, similar to the knowledge management process, can be broken down into a series of discrete, but inter-dependent, stages. Having a robust innovation process is necessary for the creation and commercialisation of intellectual assets.

5 Research methodology

For the purposes of this paper, the author used the knowledge management model (Desouza, 2006) and the innovation process (Desouza et al., 2006) as points of departure. Each of these prior studies:

- 1 spanned about two years
- 2 involved a rigorous examination of literatures from multiple disciplines
- 3 analysed data collected from interviewing over 60 executives in over ten industries and eight countries
- 4 arrived at validated models.

To examine the security challenges associated with intellectual assets, both from a knowledge management and innovation perspective, the first task was to integrate these two models. The goals of the integration were to:

- 1 build a holistic model to guide the management of intellectual assets
- 2 to use the model as a guide for interviewing executives on the security challenges faced when creating and commercialising intellectual assets.

To this end, the various stages of knowledge management were mapped onto the innovation process and a list of critical capabilities was arrived at for each stage. The integrated model will be described in the next section.

Twenty-three executives, each representing their organisation, were interviewed on the security challenges faced during each stage of the intellectual asset management

model. Representative titles included: Chief Security Officer, Security Manager, Enterprise Security Compliance Manager, Risk and Security Manager and Information Security Manager among others. Each interview lasted about 75 minutes. In most cases, interviews were preceded and succeeded by examination of documents, organisational policies and even pre- or follow-up interviews with other members of staff (e.g., risk analysts, network security personnel, data privacy officers, etc.). Interviews were transcribed, analysed and then coded using accepted guidelines of qualitative research. The coding template was devised following the guidelines prescribed by Miles and Huberman (1994). Specifically, codes were constructed from the definition of each component of the intellectual asset management model and the list of critical activities under each component, hence, providing for the theoretical and conceptual basis for the coding scheme. To check for consistency in coding, it was deemed necessary to have two people code a portion of the interviews. To this end, seven interviews were coded by the researcher and another coder. Inter-coder reliability was measured by examining if the two coders had found similar concepts discussed in the transcripts and also selected similar paragraphs from the transcripts representing the concept (Miles and Huberman 1994). Computation of the inter-coder reliability was based on Miles and Huberman (1994), i.e., [number of agreements / (total number of agreements and disagreements)]. Three interviews were coded first, and then discussed, after which, four more interviews were coded. The inter-coder reliability for the coding was 0.88.

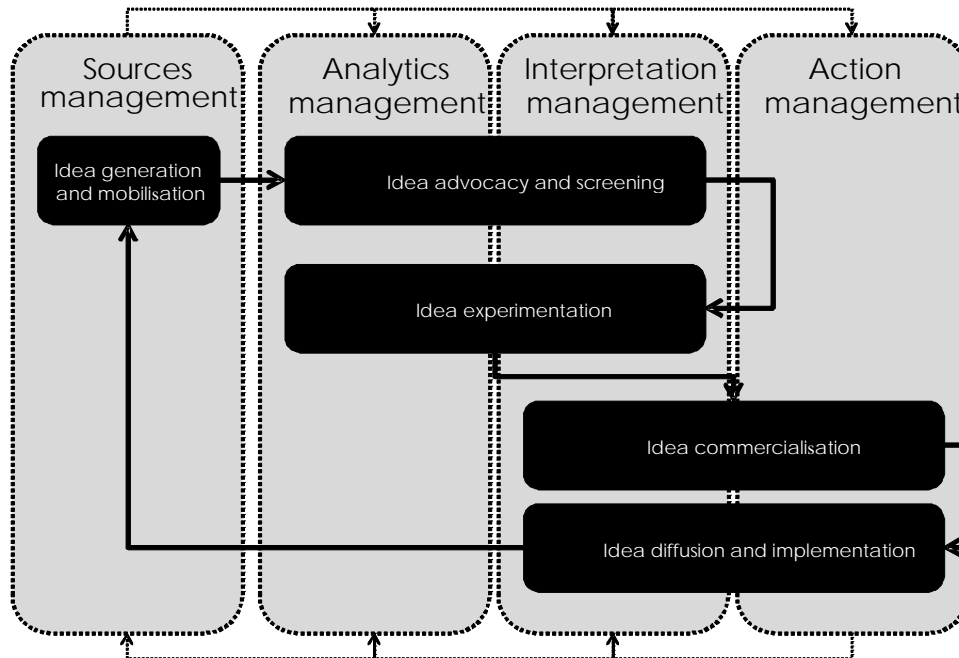
Upon completion of the data analysis, the findings were presented to the original executives interviewed for feedback and to gain face validity and make any refinements. All executives interviewed strongly supported the findings and endorsed them. The findings were then presented at several executive roundtable briefings and professional conferences where they were put through further scrutiny and refinement. Overall, the author feels confident about the validity, reliability and practicality of the security challenges associated with the management of intellectual assets that emerged through the interviews.

6 Intellectual asset management model

This paper takes the perspective that the innovation process model is the means and ends through which intellectual assets are deployed and the knowledge management model serves as a basis from which to optimise the innovation process (see Figure 2).

As noted earlier, ideas are the ingredients for the innovation process. Ideas are either created by or solicited from sources of interest; this occurs in the stage of 'idea generation and mobilisation'. As shown in Figure 2, the ideal organisation will have to show competency in conducting adequate 'sources management' if it is to be successful in idea generation and mobilisation. The capabilities described for sources management are critical when considering how ideas are generated and mobilised. For example, the capabilities of identification of sources and being able to evaluate sources are vital as they promote:

- 1 the scanning of the internal and external environments for sources that may have ideas of value
- 2 the evaluation of the credibility of the sources, which impacts the perceived quality of their ideas.

Figure 2 Intellectual asset management model

Failure to show competency in these two capabilities will result in the organisation not having an adequate grasp of its environment and the sources of ideas. Moreover, the organisation will not be able to critically evaluate sources or be able to prioritise sources from which ideas need to be considered. Similarly, without adequate information retrieval procedures, the organisation may not be able to tap into ideas from sources. For instance, use of an incorrect retrieval procedure on a source will lead to the quality of ideas getting compromised due to the retrieval procedure. Organisation of sources is also essential for:

- 1 constructing a map of sources
- 2 aggregating and integrating sources that are working in similar domain
- 3 understanding the gaps and areas of redundancy in an organisation's inventory of sources, thereby, influencing future investment decisions for new sources.

Evaluating and updating the collection of sources is critical in today's dynamic environment as new sources may emerge and current sources may become obsolete. Moreover, a given source might increase their experience and maturity in terms of expertise within a given domain, thereby, increasing their credibility and reliability for providing valuable ideas. Cases may occur where an entire group of sources (e.g., sources working on nanotechnology issues) become more valuable, or conversely, an entire collection of sources may become obsolete (e.g., sources working on Y2K problems). Finally, as noted earlier, it is important to have mechanisms to protect sources that are of high value; these sources need to be kept rare in the marketplace, so as to preserve their value and give the organisation exclusive rights to their ideas and innovation capacities.

The next two stages of the innovation process – idea advocacy and screening and experimentation – require sound analytical management and interpretation management capabilities. Seldom are ideas valuable in isolation. It is more common for ideas to be viewed in the context of other ideas and the business environment. As such, it is important to draw relationships between:

- 1 two or more ideas
- 2 idea(s) and the business environment.

The former is the domain of the analytics management, while the latter requires sound interpretation management to be able to evaluate (interpret) ideas within the context of the business environment. Relationships between ideas can help in the screening of ideas. For example, seeing patterns and trends among ideas, and being able to rank and evaluate ideas may help in screening procedures. Moreover, in order to advocate for ideas, one must know how to interpret the merits of the ideas, when compared to other ideas, in the context of the current and future business environments. In addition to the ability to generate relationships (the analytics) and assess (the interpretation) ideas, other capabilities found within the components of analytics management and interpretation management are salient. For instance, consider the capabilities of validating and visualising relationships. Unless these capabilities are present during the advocacy and screening of ideas, we may have several negative outcomes, including selection of wrong ideas, poor ability to see connections among ideas and poor development of ideas. Similarly, consider the capability of storing interpretations. The organisation should have a viable knowledge base wherein ideas can reside along with the context surrounding their evaluation. Lack of a reliable knowledge base will lead to spending time to reinvent existing ideas, inability to link current ideas with those of the past and the inability to trace and revisit past interpretation activities.

During the experimentation process, the interpretation management capabilities dominate the process, along with capabilities found in analytics management. The process of experimentation calls for the continuous testing, interpretation, refinement and re-testing of ideas. If an organisation has immature capabilities in information processing (the analytics) and sense-making (the interpretation), its experimentation process will be less than ideal. Consider the capability of having an analytics management framework. Unless an organisation has an experimentation framework, individuals will not adequately collaborate on experiments or even share results from experiments. Moreover, simply having a framework for analytics management is insufficient. The organisation must continuously seek to optimise and refine its experimentation process, thereby innovating the process and infusing it with newer analytical tools (the capability of managing and evaluating analytical tools), as necessary. Similarly, the methods used for interpretation management will need to be evaluated and updated as conditions change in the marketplace. For example, if the organisation has recently expanded globally, it may require its interpretation management methods to be updated for language, greater inclusion of new partners and increased diversity of thoughts.

During the commercialisation of ideas and their subsequent diffusion and implementation in the marketplace as products and services, it is important for an organisation to carefully consider the capabilities discussed in the components of interpretation management and action management. During these final two stages, the organisation will be judged by the actions it calibrates and executes. Unlike prior stages,

which had a greater internal component, during these final two stages, the organisation's actions are going to make clear and distinctive marks in the external environment, as the prominence of the action management capabilities comes to the forefront. The organisation must be able to calibrate appropriate products and/or services (the creation of actions), which require sound interpretation of the external environment (generating interpretations and testing interpretations). Moreover, the organisation will be required to demonstrate sound coordination capabilities (sharing interpretations and coordination of actions) in order to generate interpretations and execute actions. As the product and/or service begin to penetrate the marketplace, the organisation's learning and evaluation capabilities will play a pivotal role. The organisation will need to ensure that it can learn from its current effort and use the learning to shape future innovation efforts. Learning that occurs during these phases will serve as feedback to each of the prior stages of the innovation process. For example, if assessments of a product's reach and customer appeal were found to be incorrect, the organisation may want to assess how to improve its idea screening procedures in the future so as to avoid similar incidents.

As shown above, the innovation process draws heavily on the capabilities required for sound knowledge management. The challenge for the organisation is to not only have robust capabilities for the management of sources, analytics, interpretation and action, but also to be able to innovate and develop superior capabilities to retain its competitive advantages. Moreover, the organisation should protect the ingredients and capabilities within each component of the innovation process so as to retain competitive advantages. Through the innovation process, intellectual assets are created and commercialised, so as to secure value and competitive advantages for the organisation.

7 Managing security of intellectual assets

The intellectual asset management model outlined above was used to guide interviews with executives on the security management challenges faced by organisations. Interviewees were provided with a description of each stage of the innovation process, the critical capabilities for each stage (which were drawn from their corresponding knowledge management components) and examples of innovation programs in each stage. Examples of innovation programs were provided to give the interviewee a sense of people, process and technology-enabled activities that are normally conducted within each stage, so as to ensure that the executives:

- 1 understood each stage of the innovation process
- 2 considered all three types of activities that might occur within each stage.

For example, during the discussion of the idea generation and mobilisation stage, examples were given on how Procter and Gamble developed a program to connect with external sources to retrieve information on solutions that it cannot solve internally (Huston and Sakkab, 2006), and how Washington Mutual provides incentives to employees to share ideas with peers (Desouza et al., 2006). Similarly, during the discussion of idea experimentation, examples were provided including the use of computer-aided simulation tools at BMW (Thomke, 2003) and virtual collaboration studios used by DreamWorks (Leonard, 2006). The author will now describe the security challenges that emerged within each stage of the innovation process.

8 Idea generation and mobilisation

All executives interviewed agreed on the criticality of protecting sources of ideas. Specifically, executives were in agreement that their organisations faced great challenges in:

- 1 identifying their (most) valuable, non-obvious sources
- 2 evaluating the credibility, reliability and vulnerability of sources
- 3 moving sources from individual assets to organisational assets
- 4 protecting valuable sources from natural and human harm
- 5 removal of obsolete and rogue sources.

In terms of identifying valuable sources, the critical issue faced by executives was to move beyond the obvious sources and identify sources that are hidden. Consider the following:

“CEO, CIO, CFO, anyone who is at the C-level is a valuable source, so are their direct reports. We do have contingencies plans in place that address the (security and protection) issues for these sources. We also know how valuable each of our global client accounts are... Though we do not have control over them, we do plan for risks associated with losing each of these... But, these are known sources... In terms of innovation, a lot of times, we do not know who are our sources... is it Jack or Julie... or is it Samantha... Our firm employs well over 80,000 people in several global locations, we cannot protect all these sources... so we need to identify the ‘most’ valuable ones...”

As noted in the above comment, the critical issue is to be able to identify who are the most valuable, but non-obvious, sources. The challenge for the organisation is further complicated by the fact that the security units of firms are often disconnected from the everyday business of the firm, including most aspects of innovation. Hence, seldom do they get to see or hear of important sources of innovation. This challenge is further complicated when it comes to human sources rather than technical ones.

“Anytime we get a new database created or purchase an information system, there is a detailed security assessment and evaluation. If needed, we will construct new security protocols to ensure that the information is protected from unauthorised access and sabotage... I do not know of processes in place for our human sources... what if a given department starts placing emphasis on information it hears from a customer or what is found on a blog... we will never be consulted on these matters... We can control the technical environment fairly well, the problem lies in human space...”

In terms of evaluating sources, the challenge of conducting effective and efficient, background checks surfaced. Most executives pointed to the difficulties they faced in implementing protocols to govern how background checks were conducted. About 3/5th of the organisations examined admitted that they either do not have good processes in place for conducting background checks or overdo background checks to a point that they become an impediment to business (Desouza, 2007). Human sources bring to the organisation a great deal of information, knowledge and expertise. Moreover, it is humans that interact with the organisation’s resources and assets. Therefore, it is critical to limit the chances of rouge sources entering the organisation and sabotaging

organisational efforts. Equally important is the need to ensure that human sources who interact with the organisation meet necessary security and trustworthiness standards in order to be trusted to hold sensitive information with confidence.

Four critical issues with background checks were discussed. First, is the issue of ensuring that an organisation has an effective and efficient process whereby to conduct a wide-array of background checks. Background checks can vary in their level of detail and cost. Overly detailed checks can waste valuable time and money, resources that are better spent on training new employees. Companies who have robust background check processes know how to conduct various types of checks depending on the kind of employee that is being screened. The ideal organisation will know how to evaluate the risks posed by a human source to the intellectual assets of the firm and conduct the necessary background check against these risks. It is advisable not to give all-purpose clearances upon the completion of these checks; instead, background checks are used to vet employees for very specific tasks, projects and roles (Desouza, 2007). If the job of an employee should change, either due to lateral or vertical movements, a new check may be required to upgrade the employee's access levels.

Second, background checks are often seen as intrusive and may lead to anxiety on the part of potential and current sources. While executives recognised this issue, they felt strongly that background checks are soon going to be a standard requirement for most jobs. It is desirable to be as transparent as possible about the process of how these checks are conducted, why are they necessary and having mechanisms whereby employees can voice their concern and share feedback. For example, informing employees that being honest and upfront about sensitive information (e.g., past use of recreational drugs) is most often viewed as a positive rather than a negative. However, if such information was discovered during the check and was not submitted in advance, it could raise questions regarding the employee's trustworthiness and honesty. While being open and transparent regarding the process of background checks is important, most executives recognised that they need to preserve the secrecy of some elements of the process so as not to allow individuals to game the process.

Third, background checks are normally a static artefact in most organisations. Organisations conduct these at the time of employment or soliciting work by a contractor. However, what is needed is a more regular way to update the evaluation of sources. Several organisations are now institutionalising the process of conducting regular check-ups on employees, especially those that work in highly sensitive areas and those that hold highly significant positions. These check-ups can be considered akin to dynamic and regularly scheduled background checks and risk profile estimation through the routine scanning of details such as the well-being of employees, their financial health, etc. Sources that engage in rogue behaviour or those that act under coercive pressures may come into the organisation with clean slates. However, conditions may develop after hiring that may sway them in different directions. During the annual, bi-annual or quarterly reviews, managers are being asked to rate employees on measures of trust and provide a security and risk evaluation. In some organisations, only after the employee has been vetted, displayed integrity and demonstrated that he or she follows security procedures will unsupervised access be given to sensitive intellectual assets of the firm.

Fourth, the criticality of background checks was discussed for sensitive (Human Resource Managers, Security Managers, Audit Staff, etc.) and/or senior (e.g., CEO, CIO, etc.) positions of the organisation. Security officials pointed out the need to have an

adequate understanding of the role of these positions and especially their involvements in identifying and acquiring foreign sources of interest to the organisations. As one official noted:

“I am really concerned about our human resource staff... they are our eyes and ears to the outside world... they screen potential employees, recruit new staff and even train our staff... they have a significant role in determining who enters our organisation. Any one of them could, if they wanted to, cause serious damage to our firm by either knowingly allowing rouge individuals to enter to the organisation... or even leaking sensitive firm information during the recruiting and selection process...”

Executives were also concerned with their inability to entice employees to contribute their most valuable sources to the organisational domain. In many cases, employees fail to share their most valuable information and sources. Much of this can be attributed to the fact that these are seen as sources of power and advancement in the organisation. Leaving sources at the individual level exposes the organisation to risks, as these sources cannot be protected via organisational security protocols. Consider the following comments:

“We have a ‘me’ attitude in our sales force... individual working in our marketing and sales department are rewarded on a commission basis... they hoard information... the most valuable being information on valuable sources... one of our sales (representative) stored his contact list on his USB drive... during the regular back-ups, this information was never protected... he was quite content on doing so... as he did not trust his supervisors... well, one fine day, he lost his briefcase... and guess what... the USB was lost... and so was his other material... while we recreated his (computer) image from the back-up... the most valuable information was lost...”

The final issue is one of protecting sources from harm. Here, two items were discussed. The first is the criticality of protecting technical sources from sabotage, unauthorised access and natural disasters. Security officials noted that they were comfortable with the measures in place to protect their technical sources. As one executive put it succinctly:

“We have been in the business of securing our databases, information systems, servers and every other technical gadget for decades now... we have virus protection, back-up facilities, offsite data recovery, the list goes on... The challenge is not a technical one... we have the technical answers... or someone does and we know how to get in touch with them...”

The second item was the protection of human sources. Executives were less comfortable when it came to issues of protecting their human sources. In terms of the human dimension, the provision of incentives to valuable employees so that they do not leave the organisation for competitors was found to be critical. In most organisations, the provision of incentives has been the exclusive domain of the human resource function. However, all security officials that were interviewed felt strongly that the security group could play a vital role in this regard. In some organisations, this role may fall under their competitive intelligence departments as well. The security unit, or the competitive intelligence function, has a responsibility to monitor competitive moves, one of the most critical moves being the competitor’s actions to lure away one’s workers. Some organisations have one or more ‘recruiting researchers’ or ‘recruiting and personnel intelligence analysts’ on their payrolls (Desouza, 2007). These individuals have several tasks: understanding how competitors lure away their employees; understanding the kinds of incentive schemes and offers their competitors offer and how can they match or beat

those; and how to identify potential talent in the competing firms that they would like to recruit. The security unit must be able to predict which human sources pose the highest risk of leaving the organisation and take the necessary pre-emptive measures to keep them at the organisation.

The removal of sources that lose their value is a critical function of the security unit. On the technical side, this involves overseeing and advising the IT function on regular purging of the corporate databases so as to keep the content current. On the human side, this involves handling of cases where rouge employees have been discovered and need to be removed from the organisation. Security officials were deeply concerned about building processes to identify rouge human sources upfront. This is understandable given the recent urge of unpleasant incidents such as office shooting rampages, shootings in schools and universities, etc. Consider the following case as an example (Desouza, 2007). In May 2005, seven former employees of Bank of America, Wachovia, Commerce Bancorp and PNC Financial Services Group were arrested for a scheme in which they allegedly obtained customer data that they then sold to law firms and debt-collection agencies. The account numbers and balances of 670,000 accounts were found on 13 computers seized from Orazio Lembo, the alleged mastermind, who has been charged with multiple counts of illegally disclosing data from a database and one count of racketeering. Lembo allegedly paid the bank employees for the account data, and then resold the information to some 45 law firms and debt-collection agencies. In cases such as this one, the security management function plays a vital role, from quarantining the employee, to preserving the necessary evidence, aiding the legal department to take the necessary actions or aiding human resources to make final settlements with the employees.

Most organisations noted that the need to build robust practices for removing disruptive and rouge human sources from the organisation. Failure to do so may leave the organisation liable for negligence. The critical practice discussed here was building robust reporting mechanisms whereby employees could share their concerns and report suspicious behaviours. Several organisations have created official ombudsperson positions to serve as contact points for employees to report information. In addition, organisations have dedicated spaces on their intranet portals where employees can report sensitive information anonymously. Employees need to be informed about how to report suspicious behaviour and areas of concern. This involves providing guidelines as to how to report details of the incident, how not to raise the suspicion of the suspected individual, how not to accuse any individual, how to share evidence on the suspected incident, etc. Moreover, employees need to trust the reporting system. The criticality of building employee trust with the security function and the reporting system cannot be overstated. One interviewee summarised it best:

“Our employees are our eyes and ears... there are about 30 people in the security department, there are over 3,000 employees... employees need to trust that we are looking out for them and our job is to ensure they have the most secure environment in which to work in... we cannot see everything or hear everything... we need to be informed about areas in the organisation that need our attention. Employees must trust us in order to come to us with sensitive matters... no employee enjoys talking about their co-worker who they like or collaborate with... we need to be seen as a safe place, a trustworthy group and be able to hold and treat the information shared with us in the strictest confidence and attend to the matter in the most discrete manner thereby protecting all parties”.

9 Idea advocacy and screening

In the stage of advocacy and screening, fewer security challenges arose in comparison to the previous stage. All security executives pointed out that since the medium through which ideas are screened, developed and analysed are heavily technology dependent (e.g., intranet sites to collect ideas and evaluation, PowerPoint presentations to advocate for ideas), securing analytical routines and technology devices was critical. Three security challenges that did arise were:

- 1 ensuring the security and integrity of analytical tools
- 2 ensuring integrity in the application of the analytical tools
- 3 securing technology devices.

The first issue, ensuring the security and analytical tools can be considered akin to the challenge of securing information systems. Information systems are used to enable decision-making in organisations. If the analytical routines used within these technologies were ever compromised, the cost to an organisation would be severe. In 2000, an analytics management software ‘glitch’ at Nike resulted in damages to the company that ran in excess of \$100 million in lost sales, which in turn depreciated the company stock price by 20% and resulted in a number of class action lawsuits brought against the company by shareholders who believed management had been negligent in matters related to knowledge management (Koch, 2004). The glitch occurred because the ERP system used by Nike – i2’s Predictive Demand Application module – was not properly integrated with the Supply Chain Planner, as the two applications used different business rules and stored data in different formats. This lack of integration produced an incorrect forecast for shoe demands – too many orders for Air Garnetts and too few orders for Air Jordans. The situation was further exacerbated as the company’s financial records, which were connected to the accounting system, were simultaneously receiving incorrect data from the order processing system. As a result, faulty forecast predictions were reflected in balance sheets that were released to the financial media. Obviously, these conditions, in their totality, reflected poorly on the company’s business reputation. Interviewees noted that the most common practice to secure the analytical process was evaluating the software code and protecting it. Ensuring that only authorised individuals can make changes to the code and that robust protocols are in place to ensure issues of version control, backups and error checking were seen as critical practices. Also, ensuring that only authorised individuals accessed information systems was also discussed. These practices have been discussed in the computer science and information systems security literatures (Soper et al., 2007; Park et al., 2006; Boella and van der Torre, 2006; Memon and Daniels, 2007) and, therefore, will not be elaborated on here.

The second issue, of ensuring integrity in how analytical routines are applied, is very important when it comes to the management of intellectual assets. Analytical routines do represent intellectual assets of the organisation. Knowledge is encoded in these routines and knowledge is required in order to appropriately apply these routines. Moreover, these routines might represent intellectual assets that provide the organisation with competitive advantages. Consider the following statements by a Chief Security Officer:

“We are in an information rich business... 99.999% of all information that we analyse is available publicly... the .0001% of information that is not found in the public domain can be easily acquired with minimal cost through private

vendors... so what gives us the edge... it is the ability of our analyst to come up with the most creative (financial) models and predict the future... this is where we make our money... so absolutely, I do not want anyone misusing the spreadsheets and algorithms of our analyst... we will have to close down if these were ever compromised.”

In some industries, for example, the financial sector, all firms have a level playing field in terms of information access. Moreover, the use of private sources (for example, insider information) is not permitted. The success of the organisation lies in its ability to develop analytical routines that are innovative, and rare, in the marketplace. Hence, it is important to secure these intellectual assets. Securing the analytical routines must account for:

- 1 ensuring that no one from the outside can access and compromise these assets
- 2 ensuring that within the organisation these assets are deployed appropriately.

As noted in the previous paragraph, the first issue is easily handled through traditional information security measures. The second issue, however, requires more discussion.

Consider the following case of Claire, who was a product development specialist in a high-tech company.

“She had access to the company’s intellectual assets in the form of presentations, past sales documents, marketing plans, etc. In her job, she was responsible for securing new business by engaging with customers, both current and potential. However, Claire was not an expert in all aspects of the company’s products, such as product capabilities and engineering details. Claire was more of a salesperson: she specialised in managing client-relations. One day, in an attempt to quickly prepare a presentation, she decided to re-use an existing presentation on the company’s intranet site. She copied and pasted the name of the clients she was presenting and quoting to into the original presentation. In her haste, she forgot to check the presentation and e-mailed it right away to the client. Unknown to her was that the person who originally created the presentation had inserted extensive notes and details about the original client for whom the presentation had been created. Now, all of this material was compromised. Not only did Claire lose the business deal, but her organisation ended up being sued for breach confidential information. This is an example of misuse or sloppiness in how an analytical routine (in this case a presentation) was misused.” [Desouza, (2007), pp.30–31]

To protect against these situations, many organisations are now placing added security around their most valuable analytical routines. In some organisations, only after an employee has gone through training on how to use the analytical routine is access provided. In several consulting organisations, only after a consultant has completed training and received explicit permission from the creator of an intellectual asset (e.g., a presentation), may the individual use the asset. Moreover, access to use the intellectual asset is provided for a restricted and specific purpose. In other organisations, there are policies and protocols around ensuring that quality assurance. For instance, before a presentation or report can be mailed to an external party, it needs to be vetted by a senior manager, and in some cases, even the legal department.

Issues of securing technology devices is a critical concern for security executives, especially in the age of mobile computing, distributed work and virtual work. Security professionals are spending significant resources to educate their employees on safe travel practices. Organisations are monitoring and assessing the technology devices that travel in and outside of the organisation. Organisations are also providing training so that

employees can recognise risky and dangerous situations. Employees who travel need to have training in how to recognise dangerous situations and how to read environmental cues (Desouza, 2007). Employees who are travelling to foreign lands need, at the minimum, to have some basic language skills, to understand the cultural nuances of the place, to learn how not to draw attention to themselves, to know how to identify if they are being followed, to learn how to change their patterns during the day so as not to be predictable, etc. Employees are also being advised on how to manage intellectual assets (e.g., what can and cannot be read on an airplane) while travelling.

Since analytics management is heavily technology dependent, security officers also brought up the need to spend a great deal of effort to ensure that technology devices are handled with care and disposed of appropriately. It is common to find organisations adapting practices found in defence and intelligence organisations for this purpose (Desouza, 2007). Common practices include, ensuring sensitive information cannot be printed, tagging printouts with identifiers, destroying sensitive information printouts on a regular basis, etc.

10 Idea experimentation

In the context of experimentation, executives brought up the issue of employees having a safe place to create, dialogue and debate interpretations. Most of the security professionals interviewed, pointed to issues of:

- 1 workplace security (especially highly sensitive areas such as research and development labs)
- 2 offsite security (ensuring that adequate security measures are in place for interactions at offsite locations, e.g., hotel conference facilities, where meetings of a sensitive nature are held).

Security of spaces, physical or virtual, is critical as it enables for the creation of safe spaces where rich dialogues and creative experimentations can occur.

There has been a rise in work place violence, especially within the USA. Employees have entered their work premises and gone on shooting rampages, hurting their co-workers. From the perspective of protecting intellectual assets and securing the premises of the organisation, these acts represent one of the gravest forms of insecurity. If the employees, the core intellectual assets of an organisation, cannot feel safe and protected, the security programs are seriously flawed. Employees do not work well when they are scared and intimidated. It is important to have a friendly and safe work environment to be productive at work. Executives noted that it is important to remember that not all employee assaults result in physical altercations. Some of the most dangerous assaults can be emotional and psychological. At one manufacturing plant in the Midwest, female employees were constantly harassed with overt sexual gestures and mistreated on the job by their male counterparts (Desouza, 2007). Even more troubling, this issue was not dealt with by the management for over two years, when a select group of female workers went to the local newspaper with their story. Needless to say, the company faced a slew of lawsuits and fines and more importantly had to spend a great deal of effort cleaning up its image. These conditions make for hostile work environments and are not conducive for the sharing of ideas, interpretations and thoughts.

Security executives pointed out that a lot of security breaches happen on offsite facilities. These facilities are easy targets, as there is little security. Consider the following (Desouza, 2007): hotel maids were caught taking digital photos of business papers. The executives who were the targets of these assaults were frequent visitors to the hotel and often bragged about the work they did. The maid staff found a way to use the information to their advantage and increase their weekly earnings. In addition, offsite facilities such as hotels are open and accessible to the general public. Finally, most organisations cannot exert control over the security programs at hotels during offsite visits. This leaves organisations vulnerable to lurkers and snoopers.

Security officials are concerned with incidents such as these and are taking significant steps to manage the physical and offsite security of their organisations. Security practices include segmenting the office floors based on access to intellectual assets and different kinds of personnel. In addition to segmenting office spaces, controlling access to the office spaces is critical. Sensitive areas need to be monitored 24 hours a day, seven days a week, 365 days a year. These rooms should be fitted with video cameras to record personnel that come in and out of these facilities. Some organisations rightfully take an added step of precaution: access to these rooms is provided only if you are accompanied by one other person. Thus, there are normally two people who need to be there – one person that has work to perform and another who is there to monitor. Not surprisingly, the other person is normally a member of security personnel. Organisations are also taking great care to secure the entry and exit points.

An adequate security program for intellectual assets will also have plans in place to protect assets when they are outside the traditional physical confines, such as of those of the office. As noted, breaches of intellectual assets can happen quite easily during offsite meetings. The security team plays an active role in vetting the offsite locations, ensuring that adequate measures are in place to protect both the human and technical assets of the organisation during these visits and ensuring that the environments are conducive to conduct business (e.g., secure internet connections, business centers, etc.). Moreover, in the cases of global meetings, the security team will even be involved in planning logistics, such as how to get the meeting attendees to and from the facilities, dinner activities, etc. As discussed earlier, the need to build adequate reporting programs where employees can report early signs of workplace trouble and/or offsite facility issues was also brought up again. Similarly, during the conduction of an offsite meeting, especially those of a highly sensitive nature, it is important for security professionals to be alerted to early signs of concern. Building trustworthy reporting mechanisms and acting with diligence on early signs of security concerns will help limit the escalation of incidents.

11 Idea commercialisation

In terms of security issues that pertained to the stage of idea commercialisation, security executives were concerned with:

- 1 the security of sensitive communications and conversations that lead up to the release of a new product and/or service
- 2 the need for having robust counterintelligence programs to prevent and investigate leaks of sensitive information.

Interviewees discussed the need to build secured meeting spaces (e.g., conference rooms) and protocols that govern where sensitive conversations should take place. In designing an office, one of the most important design considerations involving security personnel are the meeting rooms. Best practices dictate that meeting rooms be, at the minimum, soundproofed. In this way, no one outside a meeting room can eavesdrop. It is also advisable to distinguish meeting rooms with a higher level of security. One organisation reported that it has meeting rooms specifically designated for sensitive conversations. In these meeting rooms, there are no windows, no electronic equipment is permitted and there is a person outside monitoring traffic around the meeting, among other sorts of precautions.

In addition to building secure physical spaces for sensitive conversations, executives pointed to the issue of providing a secure cyber infrastructure to protect sensitive electronic communications. In order to secure electronic communication channels, organisations must ensure that the right messages are being passed via these channels. Having clear-cut guidelines on what material can and cannot be passed through a given communication channel was noted as being important. Some organisations have protocols, which employees must follow when writing the subject of an e-mail. The subject line might contain the level of sensitivity of the e-mail (e.g., classified or secret). Some other organisations take the additional measure of creating two networks. An internal network is used to send material within the organisation, while the external network gets the message to those outside the organisation. Messages sent on the external network are monitored more closely and most often need to be cleared before they are transmitted. The use of automated technologies to parse the language of e-mails and to identify sensitive material is also becoming more common. Once these e-mails are identified, they are sent to the security department for clearance. Should the security department need more information, it can get in touch with the sender. Having clear-cut protocols on the kinds of messages that can be communicated, how messages should be structured and the process for evaluating messages over electronic channels is very important (Desouza, 2007).

Leaks and sabotages can prove to very costly for an organisation. As one interviewee remarked:

“We spent months planning for the hiring two very talented individuals... these individuals were being lured away from established players in the industry... But to our surprise and frustration, the news of this effort leaked... within 24 hours we not only lost any chance of bringing these two individuals into the company... but had resignations from four of our senior executives... a very costly leak!”

In the above case, the firm's mission was to recruit executives for senior position vacancies at their client firms. To the firm, the act of commercialisation was centred on ensuring that their target executives could be lured away from their current firms to take on new positions at their client firms. The managers who resigned from the abovementioned organisation took with them 50+ years of collective experience. The organisation not only felt the immediate dire consequences of these losses, but also from a long-term perspective, as these managers took with them several clients and the goodwill they had built up with the firm's external stakeholders, which was equally, if not more, expensive. While historically, counter-intelligence functions have been the exclusive domain of governmental organisations, especially with organisations involved

in the defence and national security arena, they are now making headway in the private sector. Consider the recent case of Hewlett Packard.

“At the annual Hewlett-Packard Board of Directors meetings in 2006 and 2005, one board member released detailed business plans to CNET news.com. This reduced HP’s competitive advantage, as it made public what was once private company information. The leak persisted for over a year. Finding the source of the leak was a priority for former CEO Carly Fiorina as well as former CEO Patricia Dunn. During their respective terms as CEOs, Fiorina and Dunn authorised private investigators (PIs) to find out who had caused the leak. During the course of that investigation, the PIs followed several common practices, physical surveillance: the PIs followed HP Board members surreptitiously; e-mail surveillance: the PIs embedded tracing mechanisms in e-mails to see if board members forwarded sensitive information; pre-texting: The PIs pretended to be other people in order to get access to phone records.” [Desouza, (2007), p.19]

For the most part, in developing counter-intelligence programs, the private sector seems to be taking its cues from their governmental counterparts. In several of the organisations studied for this research, personnel hired to manage counterintelligence efforts had experience in the government sector. The critical challenge discussed when building and managing counterintelligence programs was balancing legal and ethical considerations. As noted by an executive:

“No one likes to be the subject of these investigations... but the reality is that leaks do occur... most headlines in the press are stories that have the infamous ‘highly placed official talking under promise of anonymity’ ... If I had my way, I would not have any member of our organisation talk to the press and severely reprimand and even fire anyone that leaked information... because of a few bad apples we need to keep our counter-intelligence function in existence...”

12 Idea diffusion and implementation

In the context of diffusion and implementation, executives were fairly silent regarding the security challenges faced in the context of intellectual assets. As noted by one executive:

“At this stage of the game... the assets are out there... they are being consumed and manipulated by our customers... we have limited control over this stage... I would even say that trying to impose security controls at this stage will backfire as it might piss off our customers... customers want to use our products and not want any security overheads and headaches...”

Similar comments were echoed by other interviewees. The only practice that surfaced during the discussions was having appropriate contractual agreements to secure how intellectual assets were implemented. Consider the following comments:

“This is the stage where our legal team plays a major role... they iron out the contracts, the disclosure agreements... the parameters by which we will conduct installations, maintenance and upgrades... even when and how the products can be customised by our clients...”

In terms of crafting agreements that govern how the products and services can be used, the critical issue noted was ensuring that the organisation retains ownership over its intellectual asset. Furthermore, especially in the context of complex products and services, it is important to ensure that intellectual assets of business partners

(e.g., trademarks) are protected as well. If an organisation has utilised components from its business partners, it must do its part to protect these as well in the end-user agreements. In cases where breaches to these agreements occur, the security department plays a vital role in investigative efforts, as noted by the following comments:

“We had a situation where the books (we publish) were being scanned and sold electronically on a Chinese website... we also find complete PDF copies of books on this site... We were immediately called in to investigate... Our first priority was to coordinate with our legal team, who were devising legal action... Not only did we find the source for the PDF leaks, unfortunately it was one of our own employees, but we also managed to coordinate with other publishing houses whose books were being sold through the site and close down the website...”

13 Discussions

The research presented in this paper is exploratory and further research is needed to refine the list of security management practices in each component. Security management practices need to be evaluated from a cost-benefit perspective as well. Simply put, the security management practices must be balanced against the risk of curtailing innovation. The innovation process must thrive under security measures. Each of the practices described in this paper needs to be contextualised to meet the innovation needs of the organisation. Failure to adequately analyse the cost and benefit of each practice in terms of their effects on innovation and intellectual assets will lead to a flawed security program.

Moreover, each of the security practices described in this paper can be further analysed to uncover critical success factors of how to deploy and implement them in organisations. For instance, consider the challenge of knowing what sources of ideas to protect in terms of their competitive value. A critical method that found support when considering how to differentiate sources for their value propositions is the application of the resource-based view framework (Barney, 1991). The resource-based view of the firm provides a lens through which to examine and isolate the resources in the organisation's collection that can lead to sustained competitive advantages. Particularly valuable resources are those that are rare, heterogeneous, immobile and non-substitutable. Unless the resource has some valuable proposition, it is of no use to the organisation. Once it is determined valuable, assessing if the resource is rare in comparison to those possessed by competing firms becomes important. Particularly, is the resource heterogeneous and immobile? Unless a firm possesses a resource scarce in the industry, the resource will not be a source of sustained competitive advantage. Immobility also provides a salient resource test. Unless a resource is immobile, other firms in the industry can easily acquire the resource of interest. Mobile resources can only provide a temporary competitive advantage. The final question is whether the resource has substitutes. If the resource has substitutes than its value proposition is impaired since, there are other resource candidates if needed. However, if the resource of interest has no perfect or close substitutes, than the resource can be considered as highly significant and valuable. The resource-based view can be applied to segmenting intellectual assets in organisations (Desouza and Awazu, 2005).

The proposed security management framework can also be used to guide organisations in how resources are invested to bolster intellectual asset security programs. Securing the inputs, process and the outputs of intellectual asset management program is critical as these may all be sources of competitive advantages. Consider the case of a newspaper firm or a book publisher. The ‘sources’ used in a story or authors, who are sources for the books produced, are the true sources of competitive advantages. The process of printing, pricing, marketing and distributing books is not differentiable across firms nor is a secret. The security management resources of these firms need to carefully address how to protect these sources (the inputs). Without adequate protection, the organisations would lose the very entities that provide them the information, which is further refined through the knowledge management process, to result in outputs (e.g., books, reports, etc.). Now, contrast this with a management consulting firm, where most individuals working in these firms have comparable skills, expertise and knowledge (e.g., compare firms such as Accenture, KPMG, Boston Consulting Group). Most of these firms recruit from the same business schools and tap into similar knowledge bases; however, what differentiates these firms is their ability to ‘leverage’ these sources to meet the needs of their clients. Here, the processes of innovation are critical and will drive value more so than any single source of ideas. How the firm transforms the expertise into outputs (e.g., new business models) to advance their customers’ interest is important. Not surprising then is the fact that most of these consulting firms spend a significant amount of their resources to invest in research and development. Merely having knowledge resources is not enough. A firm may spend an inordinate amount of resources to hire the brightest individuals and pay them hefty salaries, but if the firm cannot get these individuals to collaborate and create products and services of value to the marketplace, the investment in the knowledge resources will not payoff. Hence, the focus of the security management program will be quite different for management consulting firm compared to a book publisher. The security management program should be cognisant of which component of the intellectual asset management process is truly the most valuable, and secure it first, before focusing on areas that are not critical in terms of preserving and building competitive advantages.

14 Conclusions

This paper described a framework to guide the management of intellectual assets. The framework combines the innovation and knowledge management perspectives, and can be used to trace the construction and commercialisation of intellectual assets. The framework was used to elicit critical security challenges within each stage of the intellectual asset management model. Securing intellectual assets is a critical capability for any organisation to master. Failure to secure intellectual assets can leave an organisation vulnerable to a number of negative outcomes. The ability to secure the intellectual assets of an organisation rests on the organisation’s ability to understand the process whereby these assets are created and used.

Acknowledgements

This paper draws heavily from three sources:

- 1 the author's doctoral dissertation
- 2 the Leveraging Ideas for Organizational Innovation project funded by the Institute for Innovation in Information Management (I3M) at the University of Washington
- 3 from the author's book, *Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets* (Kogan Page, 2007).

The knowledge management framework presented in this paper was developed as part of the author's doctoral dissertation. The author thanks his doctoral dissertation committee members for their valuable comments during the construction of the knowledge management model. Collaborative work with Peter Baloh, Yukika Awazu, Caroline Dombrowski, Jeff Kim, Sridhar Papagari and Sanjeev Jha, during the Leveraging Ideas for Organizational Innovation project is gratefully acknowledged. The author would also like to acknowledge the contributions from all executives who participated in the interviews, case studies and shared constructive comments on prior versions of his doctoral dissertation, the innovation research project and book manuscript. Partial funding for the research was received from I3M. This paper was prepared while in residence at the University of the Witwatersrand in South Africa. Helpful comments for revision were also received from the two anonymous reviewers and the special issue editor, Dr. Sangkyun Kim. All errors and omissions are solely my responsibility.

References

- Alavi, M. and Leidner, D.E. (2001) 'Knowledge management and knowledge management systems: conceptual foundations and research issues', *MIS Quarterly*, Vol. 25, No. 1, pp.107–136.
- Argyris, C. and Schön, D.A. (1978) *Organizational Learning: A Theory of Action Perspective*, Addison-Wesley, Reading, MA.
- Barney, J.B. (1991) 'Firm resources and sustained competitive advantage', *Journal of Management*, Vol. 17, No. 1, pp.99–120.
- Becker, E., Buhse, W., Günnewig, D. and Neils, R. (Eds.) (2003) *Digital Rights Management: Technological, Economic, Legal and Political Aspects, Lecture Notes in Computer Science*, Springer, New York, NY, Vol. 2270.
- Berger, P. and Luckmann, T. (1967) *The Social Construction of Reality*, Doubleday, Garden City.
- Bertino, E., Khan, L.R., Sandhu, R. and Thuraisingham, B. (2006) 'Secure knowledge management: confidentiality, trust and privacy', *IEEE Transactions on Systems, Man and Cybernetics, Part A*, Vol. 36, No. 3, pp.429–438.
- Boella, G. and van der Torre, L. (2006) 'Security policies for sharing knowledge in virtual communities', *IEEE Transactions on Systems, Man and Cybernetics, Part A*, Vol. 36, No. 3, pp.439–450.
- Boland, R.J. and Tenkasi, R.V. (1995) 'Perspective making and perspective taking in communities of knowing', *Organization Science*, Vol. 6, No. 4, pp.350–372.
- Chesbrough, H.W. (2003) *Open Innovation: The New Imperative for Creating and Profiting from Technology*, Harvard Business School Press, Boston.
- Cohen, D. and Prusak, L. (2001) *In Good Company: How Social Capital Makes Organizations Work*, Harvard Business School Press, Boston.

- Daft, R.L. and Lengel, R.H. (1986) 'Organizational information requirements, media richness and structural design', *Management Science*, Vol. 32, No. 5, pp.554–571.
- Daft, R.L. and Weick, K.E. (1984) 'Toward a model of organizations as interpretation systems', *Academy of Management Review*, Vol. 9, No. 2, pp.284–295.
- Daft, R.L. and Wiginton, J. (1979) 'Language and organization', *Academy of Management Review*, Vol. 4, No. 3, pp.179–191.
- Davenport, T. and Grover, V. (2001) 'Special issue: knowledge management', *Journal of Management Information System*, Vol. 31, No. 1, pp.7–10.
- Davenport, T.H. and Desouza, K.C. (2003) 'Re-using intellectual assets', *Research Note*, Institute for Strategic Change, Boston.
- Davenport, T.H. and Prusak, L. (1998) *Working Knowledge: How Organizations Manage What They Know*, Harvard Business School Press, Boston.
- Davenport, T.H., DeLong, D.W. and Beers, M.C. (1998) 'Successful knowledge management projects', *Sloan Management Review*, Vol. 39, No. 2, pp.43–57.
- Davenport, T.H., Thomas, R.J. and Desouza, K.C. (2003) 'Reusing intellectual assets', *Industrial Management*, Vol. 45, No. 3, pp.12–17.
- Desouza, K.C. (2006) 'Knowledge management maturity model: theoretical development and preliminary empirical testing', unpublished Doctoral thesis, University of Illinois at Chicago, Chicago.
- Desouza, K.C. (2007) *Managing Knowledge Security: Strategies for Protecting Your Company's Intellectual Assets*, Kogan Page, London.
- Desouza, K.C. and Awazu, Y. (2005) 'Segment and destroy: the missing capabilities of knowledge management', *Journal of Business Strategy*, Vol. 26, No. 4, pp.46–52.
- Desouza, K.C. and Hensgen, T. (2005) *Managing Information in Complex Organizations: Semiotics and Signals, Complexity and Chaos*, Armonk, M.E. Sharpe, Inc., NY.
- Desouza, K.C. and Vanapalli, G.K. (2005) 'Security knowledge in organizations: lessons from the defense and intelligence sectors', *International Journal of Information Management*, Vol. 25, No. 1, pp.85–98.
- Desouza, K.C., Dombrowski, C., Awazu, Y., Baloh, P., Papagari, S., Kim, J.Y. and Jha, S. (2006) *Crafting Organizational Innovation Processes*, Institute for Innovation in Information Management, The Information School, University of Washington, Report number: #I4I-I3M-InnovProc-1.
- Dobbertin, H., Rijmen, V. and Sowa, A. (Eds.) (2005) 'Advanced encryption standard – AES', *Lecture Notes in Computer Science*, Springer, New York, NY, Vol. 3373.
- Economist, The (2002a) 'Chain reaction', *The Economist*, Vol. 362, No. 8658, pp.13–15.
- Economist, The (2002b) 'Computers of the world unite', *The Economist*, Vol. 362, No. 8658, pp.19–20.
- Economist, The (2002c) 'Desirable dust', *The Economist*, Vol. 362, No. 8658, pp.8–9.
- Galbraith, J.R. (1994) *Competing with Flexible Lateral Organizations*, Addison-Wesley, Reading, MA.
- Garud, R. and Karnøe, P. (2001) *Path Dependence and Creation*, Lawrence Erlbaum Associates, Mahwah, NJ.
- Grant, R.M. (1996) 'Toward a knowledge-based theory of the firm', *Strategic Management Journal*, Winter special issue, Vol. 17, pp.109–122.
- Hackney, R., Desouza, K.C. and Loebbecke, C. (2005) 'Cooperation or competition: knowledge sharing processes in inter-organizational networks', in Hawamdeh, S. (Ed.): *Knowledge Management: Nurturing Culture, Innovation and Technology*, World Scientific Press, Singapore.
- Hagel, J. and Brown, J.S. (2005) 'Productive: how difficult business partnerships can accelerate innovation', *Harvard Business Review*, Vol. 83, No. 2.

- Henderson, R.M. and Cockburn, I. (1994) 'Measuring competence? Exploring firm effects in pharmaceutical research', *Strategic Management Journal*, Vol. 15, No. 8, pp.63–84.
- Huber, G.P. (1990) 'A theory of the effects of advanced information technologies on organizational design, intelligence and decision making', *Academy of Management Review*, Vol. 15, No. 1, pp.47–71.
- Huber, G.P. (1991) 'Organizational learning: the contributing processes and the literatures', *Organization Science*, Vol. 2, No. 1, pp.88–115.
- Huston, L. and Sakkab, N. (2006) 'Connect and develop: inside Proctor & Gamble's new model for innovation', *Harvard Business Review*, Vol. 84, No. 3, p.58.
- Koch, C. (2004) 'Nike rebounds: how (and why) Nike recovered from its supply chain disaster', *CIO Magazine*, 15 June.
- Kogut, B. and Zander, U. (1992) 'Knowledge of the firm, combinative capabilities and the replication of technology', *Organization Science*, Vol. 3, No. 3, pp.383–397.
- Kumar, R. and Nti, K.O. (1998) 'Differential learning and interaction in alliance dynamics: a process and outcome discrepancy model', *Organization Science*, Vol. 9, No. 3, pp.356–367.
- Langley, A. (1995) 'Between 'paralysis by analysis' and 'extinction by instinct', *Sloan Management Review*, Vol. 36, No. 3, pp.63–76.
- Larsson, R., Bengtsson, L., Henriksson, K. and Sparks, J. (1998) 'The inter-organizational learning dilemma: collective knowledge development in strategic alliances', *Organizational Science*, Vol. 9, No. 3, pp.285–305.
- Lawrence, P.R. and Lorsch, W. (1967) *Organization and Environment: Managing Differentiation and Integration*, Irwin, Homewood, IL.
- Lebson, S.J. (2007) 'Trade secrets as collateral: a US perspective', *Journal of Intellectual Property Law & Practice*, Vol. 2, No. 11, pp.726–728.
- Lee, J.-K., Upadhyaya, S.J., Rao, H.R. and Sharman, R. (2005) 'Secure knowledge management and the semantic web', *Communications of the ACM: Special Issue: The Semantic E-business Vision*, Vol. 48, No. 12, pp.48–54.
- Leonard, E. (2006) 'IT gets creative at DreamWorks', *Optimize*, April, Vol. 54, pp.54, available at <http://optimizemagazine.com/article/showArticle.jhtml?articleId=184400233>.
- March, J.G. (1991) 'Exploration and exploitation in organizational learning', *Organization Science*, Vol. 2, No. 1, pp.71–87.
- March, J.G. and Simon, H.A. (1958) *Organizations*, John Wiley, New York.
- Memon, N. and Daniels, T. (2007) 'Special issue on secure knowledge management guest editor's introduction', *Information Systems Frontiers*, Vol. 9, No. 5, pp.449–450.
- Miles, M.B. and Huberman, A.M. (1994) *Qualitative Data Analysis: A Sourcebook of New Methods*, Sage Publications, Newbury Park, CA.
- Mitroff, I.I. (1988) 'Crisis management: cutting through the confusion', *Sloan Management Review*, Vol. 29, No. 2, pp.15–20.
- Nonaka, I. (1991) 'The knowledge-creating company', *Harvard Business Review*, Vol. 69, No. 6, pp.96–104.
- Nonaka, I. (1994) 'A dynamic theory of organizational knowledge creation', *Organization Science*, Vol. 5, No. 1, pp.14–37.
- Nonaka, I. and Takeuchi, H. (1995) *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*, Oxford University Press, New York.
- Park I., Lee, J., Upadhyaya, S.J. and Rao, H.R. (2006) 'Emerging issues for secure knowledge management: results of a delphi study', *IEEE Transaction on Systems, Man and Cybernetics, Part A*, Vol. 36, No. 3, pp.421–428.
- Polanyi, M. (1958) *Personal Knowledge*, University of Chicago Press, Chicago.
- Polanyi, M. (1966) *The Tacit Dimension*, Anchor Day Books, New York.

- Ramaprasad, A. and Ambrose, P.J. (1999) 'The semiotics of knowledge management', *Ninth Workshop on Information Technology and Systems (WITS-99)*, 11–12 December, Charlotte, NC.
- Ramaprasad, A. and Rai, A. (1996) 'Envisioning management of information', *Omega: International Journal of Management Science*, Vol. 24, No. 2, pp.179–193.
- Rosenberg, N. (1994) *Exploring the Black Box: Technology, Economics and History*, Cambridge University Press, Cambridge, UK.
- Saussure, F.D. (1916) *Course in General Linguistics*, McGraw Hill, New York.
- Smith, A. [1910(1776)] *An Inquiry into The Nature and Causes of The Wealth of Nations*, Everyman's Library, New York.
- Soper, D.S., Demirkan, H. and Goul, M. (2007) 'An inter-organizational knowledge-sharing security model with breach propagation detection', *Information Systems Frontiers*, Vol. 9, No. 5, pp.469–479.
- Teece, D.J., Pisano, G. and Shuen, A. (1997) 'Dynamic capabilities and strategic management', *Strategic Management Journal*, Vol. 8, No. 7, pp.509–530.
- Thomke, S. (2003) *Experimentation Matters: Unlocking the Potential of New Technologies for Innovation*, Harvard Business School Press, Boston, MA.
- Tufte, E.R. (1990) *Envisioning Information*, Graphics Press, Cheshire, CT.
- van Wijk, J. (2002) 'Dealing with piracy: intellectual asset management in music and software', *European Management Journal*, Vol. 20, No. 6, pp.689–698.
- von Hippel, E. (1994) 'Sticky information and the locus of problem solving: implications for innovation', *Management Science*, Vol. 40, No. 4, pp.429–439.
- von Hippel, E. and von Krogh, G. (2003) 'Open source software and the 'private-collective' innovation model: issues for organization science', *Organization Science*, Vol. 14, No. 2, p.209.
- von Krogh, G., Ichijo, K. and Nonaka, I. (2000) *Enabling Knowledge Creation: How to Unlock the Mystery of Tacit Knowledge and Release the Power of Innovation*, Oxford University Press, New York.
- Walsh, J.P. and Ungson, G.R. (1991) 'Organizational memory', *Academy of Management Review*, Vol. 16, No. 1, pp.57–91.
- Weick, K. (1995) *Sensemaking in Organizations*, Sage Publications, Thousand Oaks, CA.
- Zander, U. and Kogut, B. (1995) 'Knowledge and the speed of the transfer and imitation of organization capabilities: an empirical test', *Organization Science*, Vol. 6, No. 1, pp.76–92.
- Zollo, M. and Winter, S.G. (2002) 'Deliberate learning and the evolution of dynamic capabilities', *Organization Science*, Vol. 13, No. 3, pp.339–351.