The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0968-5227.htm

Received 16 May 2011
Revised 16 August 2011,
12 October 2011
Accepted 13 October 2011

Incorporating business strategy formulation with identity management strategy formulation

Cornelius Johannes Kruger and Mavis Noxolo Mama
Department of Informatics, University of Pretoria, Pretoria, South Africa

Abstract

Purpose – Identity management (IdM) not only improves the process of creating and maintaining digital identities across business systems; it can, if implemented successfully, contribute to the strengthening and positioning of the business for success. In order to have a successful IdM implementation, an organisation must step back to determine a course of action that solves enterprise-wide issues. Short-sighted actions can lead to confusion, unnecessary expenses and the delay of beneficial results. The purpose of this paper is to deliver guidelines for the application of strategic management principles regarding IdM implementation, and propose a holistic model incorporating business strategy formulation with IdM strategy formulation.

Design/methodology/approach – A total of ten senior managers involved in IdM implementation projects were interviewed. Face-to face interviews were conducted, with 30 minutes allocated per participant, and an assistant present to administer the proceedings. Primary data was collected using a semi-structured questionnaire. Part A of the questionnaire collected the respondent's details and provided definitions of IdM to clarify the concept. Part B consisted of descriptive questions which dealt with the following three categories: IdM as part of the business strategy, IdM challenges in the company, IdM implementation approach used by the company and strategic framework used.

Findings – Findings indicate that IdM is seen as part of strategy and as such IdM implementations consist of a strategic thinking process accompanied by an incremental tactical implementation. Challenges facing IdM centred not on technological issues, but on implementing IdM as a competitive tool. Unfortunately, lack of commitment and external environment analysis; relegate IdM planning to remain on a tactical, rather than a strategic level.

Originality/value – A strategic planning process is presented in this article to model the interdependence between IdM implementation planning and strategic management (business strategy formulation). This model enables the organisation to develop and communicate its vision for IdM, to link IdM and business plans, and to gain the support of the whole enterprise in this endeavour. By leveraging the proposed model, organisations can gain a bird's eye view of IdM as an integral part of the business strategy, and ensure an IdM implementation that has enterprise-wide support and benefits.

Keywords Identity management, Business strategy formulation, Strategic management principles, Identity management guidelines, Security, Management strategy, Corporate strategy

Paper type Research paper

1. Introduction

With the advent of information technology, users' roles in information systems have evolved from IT specialists for access information facilities, to non-IT personnel for regular operations, to unspecified individuals from outside (Hong *et al.*, 2003, p. 243).

The authors would like to thank attendees of the 16th Americas Conference on Information Systems (AMCIS' 2010), 12-15 August 2010, Lima, Peru, for their constructive suggestions to improve this paper.

Information Management & Computer Security
Vol. 20 No. 3, 2012
pp. 152-169
© Emerald Group Publishing Limited
0968-5227
DOI 10.1108/09685221211247271

المنارة للاستشارات
www.mana

Due to the serious threat of unauthorised users gaining access to restricted systems over the internet, information security is facing unprecedented challenges (Eloff and von Solms, 2000a, b; Eloff and Eloff, 2003). The emergence of web-based technologies and the increase in remote access through mobile devices enable enterprises to extend their perimeters beyond corporate firewalls. Opening access to enterprise network systems unfortunately introduces the complexity of dealing with a growing number of user identities and managing their rights within specific company systems (Microsoft, 2002; Securitytech.com, 2004). Failing to manage identities can easily lead to the compromise of enterprise security or the exposure of sensitive information. Delivered via a set of processes and tools to create, maintain and terminate digital identities, identity management (IdM) provides the ability to identify users, applications or devices across the organisation and even beyond its borders. It automates processes and specifically addresses security processes associated with establishing adequate internal controls around financial reporting in particular (Sun Microsystems, 2004).

Unfortunately, as Fuchs and Pernul (2007, p. 1) note, "IdM has not gained comparable significance within the research community"; they continue, stating that "our engagement in different IdM projects has revealed the need for careful planning and a modularised introduction of an in-house IdM Strategy and Infrastructure". Similarly, Hong *et al.* (2003) warn that although there is plenty of security technology research, due to the lack of IdM theory, few empirical studies have been conducted to examine the effectiveness of managerial strategies and tools. Hong *et al.* (2003) therefore emphasise that security should deal not only with the integrity and confidentiality of data and information, but should also embrace managerial aspects such as the combining of security systems and defining operational procedures.

Problem statement

Dhillon and Backhouse (2000) argue that in the new millennium, it is ever more important for organisations to understand the respective roles and responsibilities of managerial structures and the role of planning. In order to manage information security effectively, a comprehensive IT security program should be established (Von Solms, 1999). Apart from specifying that the main elements of such a program should include:

- Corporate IT security policy.
- IT system security policy.
- IT security plan, Von Solms (1999) stresses that the roles and responsibilities of managers should be well-defined.

Von Solms (1999) proposes the establishment of an IT security forum (to provide directives and standards) and an IT security officer (acting as the focus of all IT security aspects) to guide successful implementation. In proposing that organisations decide on an element of strategy to manage information security, Von Solms (1999) touches on the formulation of an information technology (IT) steering committee and an IT security forum, comprising both IT representatives and end-users. Unfortunately, von Solms does not specify how or by whom these structures should be formulated. In emphasising the formulation of "Vision" and "Strategy" as the first elements in the preparation of IT security measures, Vermeulen and von Solms (2002) stress the need for buy-in by top management to security management, for which they

المنارة للاستشارات

www.mana

are ultimately responsible. In other words, organisations need a methodology that provides explicit steps, which are part of a structured and integrated process.

James (2004) argues that in today's competitive business environment, it has become crucial for enterprises to engage in more than security issues; in particular they should address strategic planning in preparation for IdM implementation. Dealing with IdM in isolation from the overall business strategy results in fragmented solutions, failure to deliver real business value, and failure to leverage existing investments and infrastructure (Vanamali, 2004). The effect is a dilution of IdM initiatives over time, making it increasingly difficult to find funding for further initiatives.

In illustrating the problems surrounding a failure to manage IdM strategically, Dixon (2005) refers to a particular company that launched competing IdM projects. These were two different projects with two different technologies, and neither team within the company knew about the other. This situation caused two factions within the same company to use IdM manoeuvres for political gain. When IdM implementation planning is not incorporated within the business strategy, teams within the company do not strive towards a common goal. These often result in negative outcome for business as a whole. Fuchs and Pernul (2007) concur that human factors and political agendas play an important role in the process of IdM policy definition and consolidation. IdM implementation often involves a "reinvention of the wheel" with money being spent on different technologies, all of which produce similar results. To address some of these issues, Vanamali (2004) provided an IdM framework that guides the establishment of a high-level roadmap for the implementation of strategic IdM initiatives. This framework not only provides guidance for the establishment of tactical processes, it also considers the impact of IdM implementation on the organisation's structures, policies, practices and technology platforms. In a similar manner, by placing emphasis on organisational aspects rather than taking a technical approach, Fuchs and Pernul (2007) developed a structured, process-orientated methodology for introducing an IdM infrastructure. After implementing their approach in a number of organisations, Fuchs and Pernul (2007, p. 8) concluded that IdM is an intensive and time-consuming "political" task, due to the need for different stakeholders to agree upon standardised workflows.

Apart for the models, guidelines and frameworks proposed by Vanamali (2004), Eloff and von Solms (2000a, b), Vermeulen and von Solms (2002) and Fuchs and Pernul (2007). The literature, for most part, neglects to supply a holistic model that incorporates IdM strategy formulation with business strategy formulation. This leads business decision makers to consider IdM as being an issue separate from business strategy formulation. This inability to formulate a generic model depicting IdM as an integral part of business strategy can be, to a great extent, attributed to:

- a lack of knowledge with regard to security management concepts;
- an inability to recognise the strategic value of IdM; and
- a failure to understand the impact of the different models of business strategy formulation (strategic management) on IdM implementation.

There is thus a need to formulate a generic model that highlights the interdependency between IdM strategy formulation and strategic management (business strategy formulation).

المنارة للاستشارات

www.mana

Objectives

This article aims to deliver guidelines for the application of strategic management principles regarding IdM implementation, and proposes a holistic model incorporating business strategy formulation with IdM strategy formulation.

2. Security management concepts

In reviewing internationally accepted information systems (IS) and information and communication technology (ICT-related guidelines, standards, codes of practice and certification (COBIT, BS7799, C:CUR 98, PENT 99), Eloff and von Solms (2000b) try to clarify the often confusing security management concepts and definitions. These authors propose a hierarchical framework for the management of IT and ICT, and highlight the difference between IT/ICT for general use and IT/ICT that deals with security issues. Within the realm of IT/ICT security, IT/ICT for security is defined as technology that support security processes. In contrast, Information Security Management (ISM) is seen as the area allocated to all IS managerial actions regarding information security. Building on the work of Eloff and von Solms (2000b), Hong *et al.* (2003) argue that the concept of ISM is still open to many definitions. They propose that, whereas the goal of information security is to prevent the unauthorised acts of users, ISM covers different theory and processes. Issues and concepts such as security policy, risk management, control and auditing, and contingency theory all address one or more components of ISM. Hong *et al.* (2003) are of the opinion that none of these issues/concepts cover the entire scope of ISM.

According to Fuchs and Pernul (2007), it is specifically issues such as risk management, governance and compliance that require IdM attention within ISM. Whether it is dealing with the storage, administration and usage of digital entities during their lifecycle; covering simple tasks such as automation allocation and revocation of user resources; or sophisticated duties such as role development on an organisational level; IdM is evolving into a core component of ISM (Fuchs and Pernul, 2007). Regarding issues such as risk management, governance and compliance, in order to safeguard confidential and sensitive information, companies are forced to adhere to internal controls and regulations such as the US Sarbanes-Oxley (SOX) Act of 2002, Basel II, BSI Grundschultz, Directive 95/46/EC of the European Parliament, ISO Security standards (such as ISO 27002) and other internal compliance regulations (Fuchs and Pernul, 2007). Clarke (as quoted by McCue, 2006, p. 1) states that: "In a Sarbanes-Oxley controlled environment, IdM is key". McCue (2006) argues that without a proper IdM solution, organisations will struggle to maintain compliance with these regulations. Fuchs and Pernul (2007, p. 1) agree, asserting that "IdM is seen as a main provider of compliance in modern companies". IdM is therefore often highlighted as one of the key trends affecting the IT security market (BMI_T, 2008). Unfortunately, as Buell and Sandhu (2003) warn, managing multiple versions of users' identities across multiple legacy applications is a daunting task. Without doubt, a strategic approach to IdM (authentication, administration and authorisation), and especially the implementation thereof, is drastically needed.

In addition to its emergence as a critical foundation for realising governance, risk management and compliance (GRC), IdM has become a crucial issue for sound business practice (BMI_T, 2008). Vanamali (2004) contends that IdM addresses more than just security issues, providing business value through auditing, compliance and monitoring.

www.mana

Hewlett-Packard (2006) explains that IdM tools permit selective assignment of roles and privileges, which facilitates compliance with regulatory controls and contributes to privacy-sensitive access controls. This indicates that IdM is broad in scope, covering both technological (application) and non-technological (people and processes) aspects of an organisation. More and more, IdM is being viewed as a strategic resource, which can lead to improvements in an organisation's internal processes and value chain.

IdM implementations are complex (Charavanapavan, 2007). Spencer (2005) reports IdM systems to be large and expensive to build or buy, implement, maintain and operate. The reality is that a full IdM deployment can span years, as organisations need to integrate their disparate systems and reconcile users and access (Charavanapavan, 2007).

During the late 1980s and throughout the 1990s, authors such as Abratt (1998), Stuart (1999) and Balmer (as quoted by Balmer and Soenen, 1999) proposed a shift away from visual identification, ledgers and filing systems in favour of a modernised, technologically-driven approach to IdM. At that time, the latest developments in corporate IdM research and scholarship acknowledged that a variety of strategies were needed to meet the increasing complexity of IdM. More recently, authors such as Ahuja (2003), Vanamali (2004) and Dixon (2005) concur and have emphasised the need for a more strategic approach to IdM implementation. All the above-mentioned authors propose that IdM should be treated not as a turnkey solution, but as part of business strategy formulation. They see IdM contributing to the realisation of a responsive, flexible company; IdM is therefore not a technological consideration, but rather a strategic business need. Dixon (2005) concludes that in IdM implementation, there should be a combination of direction setting (setting a vision, mission and objectives), and strategic and implementation planning for an organisation to perform effectively. McCue (2006, p. 1) agrees and points out that: "a radically new approach to IdM is needed to address increasingly complex corporate network ID and access headaches". In order to cater for emerging IdM developments, trends and evolution, organisations need to develop and communicate their vision for IdM; link IdM and business plans; and gain the support of the whole enterprise in this endeavour.

The impact of IdM on strategy formulation

Historically, one of the greatest challenges for corporate strategists has been to gain sufficient understanding of an organisation's capabilities in order to fully consider its strategic direction (Mintzberg and Waters, 1985). Organisations need to know which actions they need to take, or can take, to establish a strategy that will create competitive advantage. This, according to Kruger and Snyman (2002), is important if an organisation seeks to define and understand its industry and operating environment, identify its competitors, and determine their strengths and weaknesses in order to anticipate their moves. Regarding strategizing for IdM, this sentiment is echoed by Fuchs and Pernul who warn that given strategic business goals should regulate the usage of electronic identities and their possible actions within systems.

One of the key issues affecting IdM implementation in businesses is the continuing focus on tactical and technological aspects. According to Macehiter (2006), IdM implementation has historically focused on discrete, technology-focused means, rather than a holistic, business-focused view, thus making the successful strategic

المنارة للاستشارات

www.mana

implementation of IdM difficult to attain. Fuchs and Pernul (2007, p. 5) concur and state that: "a technical approach that neglects the management side is leading to a situation where development processes and policies remain unused and theoretical"; the same authors continue by noting that: "while on the other hand a solely management focused approach disregards central implementation issues like integration problems between different IdM modules". Fuchs and Pernul (2007, p. 5) stress the importance of a dual concept where:

> [...] the policy and management side has to set up processes, and handle organisational issues, while technology and architecture on the other hand have a focus on integrating and testing new functionalities within the IT-infrastructure.

They conclude that "in order for strategic goals to materialise, compliant policies and processes are needed to make technological measures meaningful".

Powel (1992) warns that social, economic, technological and other managerial factors have moved organisations beyond their boundaries. Arguable, this led Kotulic and Clark (2004, p. 599) to contest that attempts to identify and categorise organisations using existing techniques and technology will most likely, in future fail. In an ever-changing environment, the key to developing a model capable of moving organisations to expand beyond their boundaries, without the fear of compromising security, lies in the commitment of managerial effort to align the company's profile (core competencies and capabilities) with its external environment. According to del Álamo (2007), IdM is often the cornerstone that supports such new and profitable business models. IdM provides the means to manage and selectively disclose user-related identity information within an institution, or between several of them, while preserving and enforcing privacy and security needs (del Álamo, 2007). IdM brings to the market an opportunity for service providers and third parties within a circle of trust to share subscribers' identity information, enabling a faster service for subscribers. This indicates that IdM implementation has strengths and opportunities that can lead an organisation to achieve competitive advantage. The use of SWOT (strong points, weak points, opportunities and threats) and competitive forces analyses (such as Porter's five forces model – Porter, 1980) can therefore be very effective in determining the impact of IdM on strategy formulation.

We belief that analysis of competitive forces reveals that IdM supports strategies of differentiation, focus and cost. Examples of IdM-led differentiation can be found in large, technology-enabled companies. Through the acquisition of early entrants to the market, such companies have captured a controlling share of the IdM market. Business customers have become attached to the differentiation in products these companies offer. In large, technologically-driven companies, IdM also allows differentiation of specifically-targeted market segments, thus facilitating a more focused strategy. Through building large pools of skills and establishing long-standing trust relationships with customers, threat of competition and substitute products are decreased, resulting in justification for higher prices charged for IdM technology and services rendered. While there are strengths and opportunities in IdM implementation, there are also threats; if a below-par IdM system is chosen, the firm's security may easily be put at risk.

Before an IdM strategy is pursued, there should be an understanding of the organisation, its environment and processes, as well as an understanding of the business problem that is to be solved. In all this planning, IdM should be regarded as

المنارة للاستشارات

www.mana

an integrated part of strategy formulation (Ahuja, 2003; Vanamali, 2004; Dixon, 2005; Macehiter, 2006). With literature supplying insufficient guidelines and/or models detailing how specifically to achieve this balance, it was decided to investigate whether companies intuitively follow a strategic approach regarding IdM.

3. Case study: IdM in a large South African telecommunications company

As an employee of a culturally diverse, multinational organisation based in South Africa, one author was able to observe, first-hand, the formulation and implementation of an IdM strategy in a large South African telecommunications company (Company A). This presented the opportunity to gather and interpret information from a real-life case study of how a typical, large business organisation approaches IdM. This section provides a short historical background of Company A.

Based on operations revenue and assets, Company A is the largest communications services provider on the African continent. It is an incumbent telecommunications operator, offering services and products to businesses, residential areas and pay phone customers. The business consists of fixed line and mobile communications services. In a joint venture with Vodafone and VenFin, Company A's mobile segment hosts the largest mobile telecommunications network operator in South Africa, with a market share of approximately 56 per cent. Company A is also well known for its fixed line network operation and dominates the market with nearly five million connected fixed lines. This is accomplished by a joint venture with MultiLinks and Africa Online. Company A has endeavoured to become a world-class operation; their vision is to be a leading customer and employee-centred ICT solutions service provider. Being fully-fledged African, Company A supports a synergistic inspirational management style (a combination of euro-centric and afro-centric management styles).

Company A's business strategy is to defend and grow profitable revenues through, among other approaches, geographic expansion into fast-growing markets. The geographic reach initiative sees both internal and external users continue to demand increasing access to the company's information resources. There is thus a need to manage user access to the company network and to reduce security risks. IdM implementation supports the growth strategy of the company. Company A has to comply with the regulations of the SOX Act in terms of appropriate access to corporate information.

4. Research methodology

In total, ten business managers and IT managers were interviewed in Company A. These managers (all "senior" with regard to organisational standing) operate in the central offices (North Eastern region) and were involved in the company's IdM strategy formulation and implementation program. Face-to-face interviews were conducted, with 30 minutes allocated per participant, and an assistant present to administer the proceedings. Primary data was collected using semi-structured questionnaires. Part A of the questionnaire collected the respondent's details and provided definitions of IdM to clarify the concept. Part B consisted of descriptive questions which dealt with the following three categories:

(1) IdM as part of the business strategy.

(2) IdM challenges in the company.

(3) IdM implementation approach used by the company and strategic framework used.

المنارة للاستشارات

www.mana

5. Discussion, results and findings

The results of the primary data analysis are presented below, structured according to the three aspects of the questionnaire. These results refer to opinions during, but before completion of the company's IdM strategy formulation and implementation program.

IdM as part of the business strategy

The response to the first question, as to whether the respondents would describe IdM as part of the company's business strategy, was in the affirmative for eight of the respondents. Two of the respondents saw IdM as only a security measure and nothing more; they did not see any link between IdM and business strategy. The respondents who answered positive regarding question one (1), also responded positively to the question "does the company consider IdM as a critical element supplying competitive advantage?". These eight respondents also acknowledged that IdM was regarded as a risk management strategic plan approved at board level, and indicated that IdM formed a key element in the fulfilment of the company's strategic vision and mission statement. Of interest is that no respondent mentioned the use of a documented process incorporating IdM strategy as part of Company A's business strategy.

IdM challenges in the company

Respondents' feedback regarding identity challenges were as follows: all ten respondents agreed that multiple user identities must be managed; eight believe there was poor operational efficiency in administering user access to multiple systems such as the network, e-mail, intranet, enterprise resource planning, and mainframe; nine agreed that user provisioning processes were inefficient; seven believe there was a lack of user validation; and nine of respondents agreed that high password reset logs must be administered. All respondents agreed that an enterprise-wide solution to authenticate and manage network access was a necessity. According to all respondents, Company A needed to strengthen its network access controls by providing strong authentication and management of user network access, in order to be able to easily audit and prove compliance. It became apparent – and all of respondents agreed – that Company A required a solution for strong user authentication that focuses on digital IdM spanning legacy systems, and emerging authentication and authorisation technologies. These requirements led Company A to create a single IdM system that controls all users (internal and external). Every system that allows access to network based users must authenticate against the IdM system.

IdM implementation approach and strategic framework used

In trying to gain an understanding of the approach employed within the company for its IdM implementation and what framework, if any, was used as a basis for the deployment of IdM, the following was found: in contrast to the eight respondents that indicated that they considered IdM to be part of a the company's business strategy, only six respondents agreed that Company A's approach towards IdM implementation was that of a strategic-thinking process accompanied by an incremental tactical implementation. Only one respondent felt that the company used a purely strategic "big bang" approach with full implementation, while three respondents thought

المنارة للاستشارات

www.mana

the approach used was tactical (i.e. short-term and technology-focused). This strongly hinted at some managers' continuing failure to see the strategic link between IdM and strategy (business strategy formulation).

A "common strategy" was mentioned by six respondents who also agreed that Company A's approach towards IdM implementation was that of a strategic-thinking process. However, all respondents commented that an external environment analysis was not undertaken. They also agreed that IdM, as a competitive tool, was not implemented. More in-depth questioning revealed that the "common strategy" referred to by respondents was, in fact, a strategic framework used by the company as a basis for its implementation planning process. Investigated further during the planning stage, this "strategy" contained elements such as the assumptions, roadmap, tactical process and benefits for the IdM system deployment and future enhancements that were foreseen.

The results show that Company A's IdM implementation approach included internal organisational analysis (understanding the organisation's position and enhancements needed to ensure achievement of its IdM objectives). It can be inferred that a gap analysis was undertaken to review the company's processes, and where gaps were found, further analysis of the impact of IdM on the business was pursued. This included gaining an understanding of the business goals and requirements that drove the need for an IdM solution and identifying the architecture for the enterprise IdM solution. According to eight of respondents, there has, however, been difficulty in funding further initiatives and IdM enhancements. A lack of executive support has been noted by the respondents. This lack of executive support can be attributed to the limitation of a "strategy" that fails to deal with external factors (opportunities and threats) or consider the impact of IdM on the formulation of generic strategies (cost, focus and differentiation). No mention was made of a process to ensure the alignment of any new IdM initiative to enterprise requirements. This brings into question why the executive would continue to support further IdM initiatives without there being a cohesive understanding of IdM's role in the overall enterprise business strategy. We suggest that Company A still needs a clear "strategy" to govern future IdM initiatives, which can be accessed by all in the enterprise.

Even though it was found that respondents view the "strategic framework" as a strategy that can align IdM implementation to key business drivers, it is, in truth, a tactical plan. Similar to the framework proposed by Vanamali (2004), it provides only a tactical implementation planning guide. Arguably, this could account for the two of the respondents who still fail to see the need for business strategy to be coupled to all IdM implementation planning.

6. A generic IdM strategy model

The need for strategic support as a prerequisite to ICT management is well documented (DeLone, 1988; Kotulic and Clark, 2004). Similar to authors such as Ahuja (2003), Vanamali (2004), Dixon (2005) and Macehiter (2006), we believe that IdM should be regarded as an integrated part of strategy formulation. The formulation of core business strategy and supportive strategies should therefore not be seen as separate entities. For IdM to be escalated to a strategic level, it should be regarded as a core component of ISM and be integrated within the strategic planning process.

المنارة للاستشارات

www.mana

In developing a generic strategy formulation model capable of providing a bird's eye view of IdM as an integral part of a business strategy, we propose a model which comprises two elements:

(1) setting of strategic mission and objectives; and

(2) establishing strategic initiatives.

The following sections discuss these two elements and conclude with a strategy formulation model for IdM implementation.

Setting a strategic mission and objectives

The proposed model presents an iterative strategic management process for IdM implementation (Figure 1). It guides strategists to first acquire an understanding of their organisation's mission or vision and future objectives. This is followed by an assessment of the internal organisational profile (strengths and weaknesses).

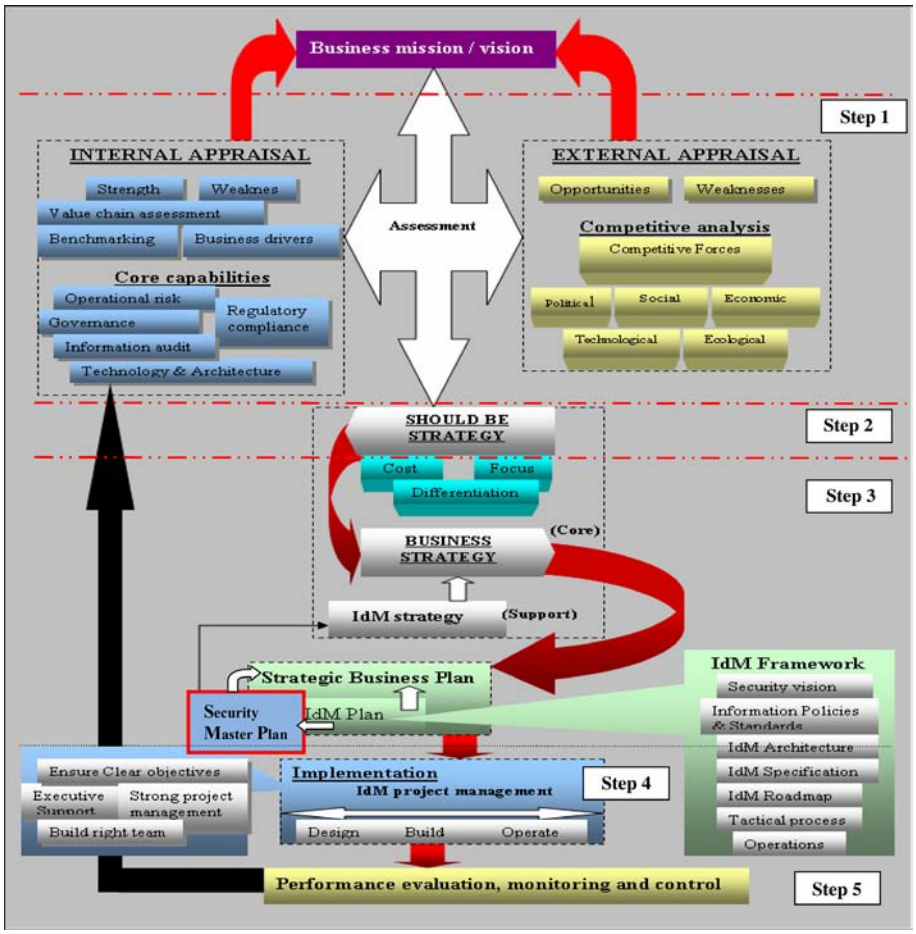

Figure 1.
The holistic strategic formulation model incorporating IdM implementation planning within the business strategy formulation process

المنارة للاستشارات

www.mana

Inventory is taken of the organisation's existing products, resources, business processes and capabilities, along with its existing plans for ISM and IdM, if any exist. The model guides an assessment of the organisation's external environment by analysing external opportunities and threats, and undertaking a competitive analysis. This enables the organisation to assess opportunities for positioning itself in a competitive market place. With this knowledge, the organisation can select the core business strategies (differentiation, focus, cost) it wishes to adopt. As IdM supports all generic business strategies, it should be seen as an enabler of any or all of these strategies.

In essence, when IdM is part of a strategy hierarchy, it should bring operational activities in line with the overall business strategy. In crafting any business strategy, the initial step of the strategic planning process is to set a clear vision, mission and objectives. These must be defined prior to crafting any IdM strategic plan. The formulation of a vision/mission/goal statements should be an organisation-wide and interactive process. All stakeholders involved should reach agreement that these statements contain goals which are attainable. During these formulation stages, social responsibility should be a critical consideration for strategic decision makers, thus vision/mission statements and future goals should express how the company intends to contribute to the societies that sustain it. Once the organisation's future vision/mission is specified, the business implications of how the organisation intends to operate in the future should be clear. The vision/mission statements governing the use of primary resource (of which IdM is one) may then be written (Kruger and Snyman, 2002).

According to Pearce and Robinson (2005) and Thompson *et al.* (2005), before pursuing an IdM strategy, organisations must understand which business problems it is trying to solve, and understand the organisational environment and processes. The creation of a vision/mission statement and identification of business objectives naturally gives rise to the need for organisations to understand their internal and external environments. As previously indicated, a SWOT analysis and Porter's five forces model (Porter, 1980) important in providing organisations with aspiring IdM initiatives a means of understanding what they need, in order to be properly positioned for the future. In the application of strategic management principles regarding IdM implementation, before setting the IdM mission/vision statements and policy, internal and external organisational assessments must take priority. Such assessments will enable the organisation to examine how the competitive environment could change in future, and how these changes should be exploited. The internal/external assessment includes the involvement of the organisation's resources and the business processes and capabilities, especially IdM processes and capabilities, in achieving the business and IdM mission and objectives. Even though we earlier implied that IdM is a strategy, IdM should also be considered to be one of the primary resources. The IdM vision/mission statement should set forth the fundamental rationale for future activities of the IdM department. This means the IdM department should be mandated to act as an enabler in ensuring the availability of appropriate information to support most, if not all, the strategic decisions of the organisation (be this from a business and/or a security perspective). This mandate should thus include the responsibility to develop the "as is" IdM architecture into the "should be" architecture, and also to develop the "future" IdM architecture needed to support the core business processes.

المنارة للاستشارات

www.mana

All these statements and architectural artefacts should form the basis for developing an organisation-wide IdM policy and an IdM strategy based on the concepts of accessibility, quality, user accountability, openness/free flow of information, security and confidentiality, privacy, cost and value, ownership/intellectual property, and misuse of information, amongst others (with reference to concepts proposed by Eloff and von Solms, 2000a, b; Hong *et al.*, 2003).

Note of clarification. Even though the formulation of an IdM strategy/policy is described separate from the overall ISM Security Master Plan (Security MP), cognizance should be taken that IdM strategy/policy should always be considered an integral part of the organisation's overall security plan. We belief the same approach described for IdM also hold true and is applicable to all other main themes of security management (control and auditing, contingency, technology, etc.);, i.e. these themes must be in line with the business strategy of the organisation. Once policy/strategy is formulated for all the main security themes, all policies/strategies must be incorporated into a single organisational wide ISM security plan consisting of appropriate policy/strategy statements or documents. This, we belief is a prerequisite to good corporate governance, the enhancement of synergy, the reduction of duplication and the elimination of perplexity. In essence, IdM policy must be combined with all other security policies and be incorporated into an organisational wide ISM policy document. The ISM policy document should contain all issues (all the main themes) regarding corporate IT security and IT system security, as proposed by Von Solms (1999).

Simultaneous assessment of the external environment (now and in the future) and the organisation's profile (as is, should be, and in the future) will enable the identification of a range of interactive opportunities regarding IdM. These opportunities provide avenues for future investment (time, money, human resources, technology). However, they should be screened through various criteria, namely the organisation's current and future vision/mission; non-negotiable policies (including aspects contained in the ISM policy); and organisational ethics, norms and values; in order to generate a set of possible and desirable opportunities. This screening process should produce a selection of options from which future strategic IdM choices may be made. It combines long-term objectives with generic strategies (cost, focus, differentiation) that position the company optimally in its external environment to achieve its vision/mission and strategic objectives. This, to a great extent, influences or determines the generic strategies (cost, differentiation, and focus) and supporting strategies (innovation, growth, alliance) the organisation will choose to adopt.

A holistic strategic formulation model

Upon completion of the initial business analysis, the proposed model guides the establishment of a high level, logical and strategic business plan to inform the actual implementation of strategy, and thus also the IdM strategy.

The IdM planning process should generate a strategic IdM plan (SIdMP) to govern the efficient and effective management and future institutionalisation of IdM systems. The SIdMP should, in a sense, be a statement of major planned initiatives, not yet defined precisely enough to be projects. The SIdMP should outline the results desired for a specific time period, as well as the major planned initiatives. After the SIdMP has been developed, the identified initiatives should be translated into a set of more defined projects with precise expected results, due dates, priorities and responsibilities.

المنارة للاستشارات

www.mana

As mentioned earlier, being part of a much larger Security MP, and business strategic plan, initiatives identified in the SIdMP must be screened against initiatives identified in the other spheres of security before prioritization can take place.

The model proposed in Figure 1 therefore superimposes the IdM tactical framework within the strategic planning phase. This enables all tactical aspects to be considered. Dixon (2005) indicates that a failure to incorporate these factors within IdM initiatives results in IdM implementation failure. The final step of the model provides for ongoing performance evaluation, monitoring and control of the implemented IdM initiatives. This ongoing monitoring takes into account changing conditions, new opportunities and new ideas that may surface. All new IdM requirements emerging after implementation will require new strategies and repetition of the business requirement analysis, planning, and implementation process. The proposed model therefore provides a bird's eye view of IdM from a business-driven perspective.

As per any business strategic plan, the IdM strategic plan (as part of the Security MP) would have to be approved, guided and monitored by the organisational executive committee and business decision makers, and communicated to all stakeholders involved. This ensures that all identified initiatives are implemented throughout the organisation, so that it can strive towards a common goal, thus eliminating the initiation of IdM initiatives that have not been approved at the top level of management.

Implementation and supporting management forums

Strategy formulation should determine direction, but it should not lose sight of how to implement the agreed strategies. In order to ensure institutionalisation of the strategy, the IdM department (as a subset of the ISM department) should be organised to support different business functions. These support structures should include regular planning and execution of IdM services, and long-term planning/direction. The modernisation of IdM services should be managed transparently, leading to IdM services being rendered congruently with business, departmental and functional priorities. Strategists and functional owners should therefore, at all times, participate in the strategy formulation process, since functional business priorities (coupled to directive, core and supportive business processes) are critical components of any strategy formulation process.

To coordinate this new "holistic" approach to ISM/IdM management, a hierarchical structure of management forums or committees should be established. In order to understand the functions and responsibilities of each forum, as well as the interaction between these forums and the various business owners, a short overview of the proposed focus and operation of each forum is presented below:

- *Corporate level forum*. The corporate ISM forum is at the top of the hierarchy and should be composed primarily of the board of directors, the chief executive and the administrative officers. This forum constitutes the highest level of executive management, and should have the final say regarding the management of security as a strategic resource in the organisation. Thus, this forum should direct the organisation's security requirements by approving not only the security system priorities reflected in SMP (and thus also the SIdMP as a subset of the Security MP), but also the required funds to realise the SIdMP as part of the strategic planning process.

المنارة للاستشارات
www.mana

- *Business level forum*. In order to service the requirements of business and corporate managers, a business forum should be established. Business owners and user system managers with specific functional responsibilities should participate in this organisational forum, to ensure that balance and focus are retained in the development of the Security MP (developed from the strategic master plans of all security related spheres). This forum, under the chairmanship of the chief information officer (or chief identity/security officer, if appointed), should carry the responsibility and authority to add value to security issues, including the IdM modernisation process, thus ensuring that the ICT department supports business and functional priorities and objectives/commitments in the provision, utilisation and maintenance of IdM systems, infrastructure and services.
- *IdM planning forum*. In order to encourage the participation of all business owners and functional representatives in the formulation of IdM planning and related policy matters, an IdM planning forum should be established. Representatives of business owners should give feedback regarding the status of their respective IdM initiatives and receive feedback regarding progress made on IdM acquisition/development work, or participate in integrating the different requirements into the SIdMP. This forum should report to the business level forum, and should be regarded as the custodians for the development of the SIdMP, to be included in the Security MP.

The successful institutionalisation of this approach to the modernisation of IdM services in an organisation will, to a great extent, be determined by the participation of all stakeholders. The IdM department, as a major role player in this strategy formulation process, should therefore ensure that the organisation is efficiently and effectively represented on all the above-mentioned forums.

7. Conclusion and recommendations

The role IdM plays in business has evolved, becoming more strategic and a critical issue, not only for security reasons, but also for sound business practice. There are increasingly strong legal and regulatory requirements governing best practice of IdM, and penalties for non-compliance can be severe. Successful implementation of IdM can therefore be a critical foundation for the realisation of GRC within the business.

IdM implementations are complex, requiring organisations to integrate their disparate systems and reconcile users and access. Best practice is, therefore, to engage in a strategic planning process in preparation for IdM implementation. As IdM is of strategic significance, capable of supporting all generic business strategies, the application of a strategic planning process allows IdM to be viewed from a business-driven perspective, as an integral part of the organisations security and business strategy. The implementation of IdM in isolation from a holistic security and business strategy results in fragmented solutions, a failure to deliver real business value, failure to leverage existing investments and infrastructure, the dilution of IdM initiatives over time, and difficulties in funding further initiatives.

A strategic planning process is presented in this article to model the interdependence between IdM implementation planning and strategic management

المنارة للاستشارات

www.mana

(security planning and business strategy formulation). The strategic planning process for IdM implementation begins with:

- the business vision;
- proceeds through gap analysis or environment assessment;
- produces a Security MP as part of the organisations business strategic plan, of which IdM is a part;
- defines business plans outlining the IdM technical and functional requirements and specifications;
- produces an IdM strategic initiatives roadmap; and
- executes identify strategic initiatives and proceeds through ongoing evaluation, management and control of the implemented strategic initiatives.

This model enables the organisation to develop and communicate its vision for IdM, to link IdM and business plans, and to gain the support of the whole enterprise in this endeavour. By leveraging the proposed model, organisations can gain a bird's eye view of IdM as an integral part of ISM and business strategy, and ensure an IdM implementation that has enterprise-wide benefits.

Our research study identified the following five steps to guide the application of strategic management principles in IdM implementations:

- *Step 1.* Understand the organisation's profile, the industry in which it operates, and its enterprise requirements.
- *Step 2.* Identify the "should be" strategy (business strategy) that IdM will support (e.g. differentiation, focus, and cost).
- *Step 3.* Create a strategic business plan incorporating IdM strategies (as an integral part of the Security MP), making use of the strategic framework to identify strategic initiatives.
- *Step 4.* Develop an implementation plan to execute the identified IdM strategic initiatives.
- *Step 5.* Establish ongoing performance monitoring and control assessments. If new requirements emerge after implementation, the process should be repeated from Step 1, including requirements analysis; strategy development; and solution planning, implementation and performance evaluation.

8. Limitations and applicability of the study

The study is limited by its focus on a single case study in a single developing country's industrial base. Given the time and logistical limitations of this study, it was not possible to include additional organisations. It was therefore decided to focus on providing insights rather than generating quantitative results. The baseline data presented should therefore be viewed as a pilot study to inform other empirical studies that investigate the perceived "enablement" afforded by IdM in business strategy, especially as it relates to developing economies. An extensive survey, and/or more in-depth case studies (e.g. 10-20 cases) are thus needed to validate the perceived benefits and confirm whether the suggested approach enhances the actual business value of organisations.

المنارة للاستشارات

www.mana

Due to the involvement of research subjects as an integral part of the research design, overly emotional or subjective involvement could have occurred due to respondents serving their own, rather than the research needs. Agreement on successful IdM might never materialise, but a long-term strategic plan for IdM implementation and policy might contribute to best practice in the field.

The line of reasoning followed throughout this article is that no single approach or model could cover all essential aspects in the arena of IdM and strategic management. The proposed model is by no means a conclusive one, or the most applicable tool in all cases when formulating a business strategy. The model simply illustrates the interdependence of strategic management and strategic IdM, and the fact that IdM is of strategic importance. It illustrates that IdM should be an integral part of business strategy.

The management of IdM, in all its complexity, constitutes much more than the issues identified in this research study. As the body of knowledge evolves, so the line of reasoning and the proposed holistic model will need to be updated and revised. Before the interdependency between IdM and strategy can be calculated more accurately, further research is required that takes into account the time needed for a large IdM implementation to impact on a business. Such a longitudinal study should span a number of years and include additional industries within different managerial and strategic settings.

References

Ahuja, J. (2003), "Identity management: a business strategy for collaborative commerce", *Information Systems Control Journal*, Vol. 6 No. 49, pp. 1-5.

Balmer, J.M.T. and Soenen, G.B. (1999), "The acid test of corporate identity management", *Journal of Marketing Management*, Vol. 15 Nos 1/3, pp. 69-92.

BMI_T (2008), "Increased risks fuel IT security market growth SA IT security market sizing and forecast 2006-2011", available at: www.engineeringnews.co.za/article/increased-risks-fuel-it-security-market-growth-2008-01-17 (accessed 16 February 2010).

Buell, D.A. and Sandhu, R. (2003), "Guest editor's introduction: identity management", *IEEE Internet Computing*, Vol. 7 No. 6, pp. 26-8.

Charavanapavan, S. (2007), "Developing a comprehensive strategy for IdM to achieve business objectives", *Fujitsu Services 2008 Proceedings of IIR Identity Management Conference, September 2008*.

del Álamo, J.M. (2007), *Leveraging New Business Models with Identity Management – An e-learning Case Study*, available at: www.it.kau.se/IFIP-summerschool/papers/S11_P2_Jose%20Alamo.pdf (accessed 15 February 2010).

DeLone, W.H. (1988), "Determinants of success of computer usage in small business", *MIS Quarterly*, Vol. 12 No. 1, pp. 51-61.

Dhillon, G. and Backhouse, J. (2000), "Information system security management in the new millennium", *Communications of the ACM*, Vol. 43 No. 7, pp. 125-8.

Dixon, M. (2005), "Discovering identity: identity management strategy", available at: http://blogs.sun.com/identity/entry/identity_mangement_strategy (assessed 15 February 2010).

Eloff, J.H.P. and Eloff, M.M. (2003), "Information security management – a new paradigm", *2003 Proceedings of the Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on Enablement Through Technology, 17-19 September*, pp. 130-6.

المنارة للاستشارات

www.mana

Eloff, M.M. and von Solms, S.H.V. (2000a), "Information security management: a hierarchical framework for various approaches", *Computers and Security*, Vol. 19 No. 3, pp. 243-56.

Eloff, M.M. and von Solms, S.H.V. (2000b), "Information security management: an approach to combine process certification and product evaluation", *Computers and Security*, Vol. 19 No. 3, pp. 698-709.

Fuchs, L. and Pernul, G. (2007), "Supporting compliant and secure user handling – a structured approach for in-house identity management", *2007 Proceedings of the Second International Conference on Availability, Reliability and Security in Washington, DC, United States of America*, IEEE Computer Society, Washington, DC.

Hewlett-Packard (2006), *The HP Security Handbook Protecting Your Business*, available at: http://h71028.www7.hp.com/ERC/downloads/HP%20Security%20Handbook%20V2.pdf (accessed 16 February 2010).

Hong, K., Chi, Y., Choa, L. and Tang, J. (2003), "An integrated system theory of information security management", *Information Management and Computer Security*, Vol. 11 No. 5, pp. 243-8.

James, P. (2004), "Strategic management meets knowledge management: a literature review and theoretical framework", *2004 Proceedings of the 2004 5th actKM Conference in Southern Cross University, East Lismore, Australia*, available at: www.actkm.org/userfiles/File/actkm2004conf/Presentations/Paul%20James'%20Research%20Forum%20Paper.pdf (accessed 15 February 2010).

Kotulic, A.G. and Clark, J.G. (2004), "Why there aren't more information security research studies", *Information and Management*, Vol. 41 No. 1, pp. 597-607.

Kruger, C.J. and Snyman, M.M.M. (2002), "The interdependability between strategic management and the formulation of an information and communication technology strategy", *South African Journal of Information Management*, Vol. 4 No. 2.

McCue, A. (2006), "CIO Jury: businesses face ID management headache", available at: www.silicon.com/management/cio-insight/2006/09/21/cio-jury-busenesses-face-id-management-headache-39162653/ (accessed 12 January 2011).

Macehiter, N. (2006), *Identity Management: An Architectural Approach for Business Value*, available at: www.mwdadvisors.com/asset/get_asset.php?id=24&file=idm.pdf (accessed 16 February 2010).

Microsoft (2002), "Understanding the benefits and pitfalls of implementing role based access controls and the impact on your business risk requirements", *2008 Proceedings of the Identity Management Conference, September*.

Mintzberg, H. and Waters, J.A. (1985), "Of strategies, deliberate or emergent", *Strategic Management Journal*, Vol. 6 No. 1, pp. 257-72.

Pearce, J.A. and Robinson, R.B. (2005), *Strategic Management, Formulation, Implementation and Control*, 9th ed., McGraw-Hill, Boston, MA.

Porter, M.E. (1980), *Competitive Strategy: Techniques for Analyzing Industries and Competitors*, The Free Press, New York, NY.

Powel, P. (1992), "Beyond networking: the rise of the nebulous organization", *European Management Journal*, Vol. 10 No. 3, pp. 352-6.

Securitytech.com (2004), *Secure Identity Management: An Integrated Solution White Paper*, Securitytech.com, available at: www.securitytechnet.com/resource/security/authen/IEG_White_Paper.pdf (accessed 16 February 2010).

Spencer, R. (2005), *Identity Management Strategy Draft*, available at: www.e-strategy.ubc.ca/__shared/assets/IDMS-strategy-11932.pdf (accessed 15 February 2010).

المنارة للاستشارات

www.mana

Stuart, H. (1999), "Towards a definitive model of the corporate identity management process", *Corporate Communications: An International Journal*, Vol. 4 No. 4, pp. 200-7.

Sun Microsystems, Inc. (2004), *The Role of Identity Management in Sarbanes-Oxley Compliance*, available at: www.sun.com/software/products/identity/wp_identity_mgmt_sarbanes_oxley.pdf (accessed 15 February 2010).

Thompson, A., Strickland, A.J. and Gamble, J.E. (2005), *Crafting and Executing Strategy: The Quest for Competitive Advantage*, 14th ed., McGraw-Hill, New York, NY.

Vanamali, S. (2004), "Identity management framework: delivering value for the business", *Information Systems Control Journal*, Vol. 4 No. 1.

Vermeulen, C. and von Solms, R. (2002), "The information security management toolbox: taking the pain out of security management", *Information Management & Computer Security*, Vol. 10 No. 3, pp. 119-25.

Von Solms, R. (1999), "Information security management: why standards are important", *Information Management & Computer Security*, Vol. 7 No. 1, pp. 50-7.

About the authors

Cornelius Johannes Kruger is an Associate Professor at the University of Pretoria, presenting primarily post graduate courses on MBA, MEM (Masters in Engineering Management), MPM (Masters in Project Management), MIT (Masters in Information Technology), MCOM, and MPHIL programs. Apart from lecturing, he has more than 14 years managerial experience in the ICT sector. He participated in the formulation/revision of numerous organizations' strategic business plans, especially regarding ICT and knowledge as strategic resources. He holds a PhD in IT and both MBA and MIT degrees (with distinction) from the University of Pretoria. He is a member of the Association of Professional Managers of South Africa, a contributing member to the Performance Measurement Association (PMA) Cranfield School of Management – UK, and an Emerald Group Literati Club Member and Emerald author. Cornelius Johannes Kruger is the corresponding author and can be contacted at: neels.kruger@up.ac.za

Mavis Noxolo Mama is a Master's (Engineering) Student at the University of Pretoria. Her research focuses on engineering, technology and project management. Current work involves the study of identity management and security, as it relates to strategic management.

To purchase reprints of this article please e-mail: **reprints@emeraldinsight.com**
Or visit our web site for further details: **www.emeraldinsight.com/reprints**

www.mana

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

www.manaraa.com