12-2009

Towards a Knowledge Perspective in Information Security Risk Assessments – an Illustrative Case Study

Piya Shedden
Department of Information Systems University of Melbourne, p.shedden@pgrad.unimelb.edu.au

Wally Smith
Department of Information Systems University of Melbourne, wsmith@unimelb.edu.au

Rens Scheepers
Department of Information Systems University of Melbourne, r.scheepers@unimelb.edu.au

Atif Ahmad
Department of Information Systems University of Melbourne, atif@unimelb.edu.au

Towards a Knowledge Perspective in Information Security Risk Assessments – an Illustrative Case Study

Piya Shedden
Department of Information Systems
University of Melbourne
Victoria 3010
p.shedden@pgrad.unimelb.edu.au

Wally Smith
Department of Information Systems
University of Melbourne
Victoria 3010
wsmith@unimelb.edu.au

Rens Scheepers
Department of Information Systems
University of Melbourne
Victoria 3010
r.scheepers@unimelb.edu.au

Atif Ahmad
Department of Information Systems
University of Melbourne
Victoria 3010
atif@unimelb.edu.au

Abstract

Many methodologies exist to assess the security risks associated with unauthorized leakage, modification and interruption of information for a given organisation. We argue that the traditional orientation of these methodologies, towards the identification and assessment of technical information assets, obscures key risks associated with the cultivation and deployment of organisational knowledge. Our argument is developed through an illustrative case study in which a well-documented methodology is applied to a complex data back-up process. This process is seen to depend, in subtle and often informal ways, on knowledge to sustain operational complexity, handle exceptions and make frequent interventions. Although typical information security methodologies identify people as critical assets, we suggest a new approach might draw on more detailed accounts of individual knowledge, collective knowledge, and their relationship to organisational processes. Drawing on the knowledge-management literature, we suggest mechanisms to incorporate these knowledge-based considerations into the scope of information security risk methodologies.

Keywords

Information security, risk management, asset identification, knowledge protection.

INTRODUCTION

Information security is of paramount importance in organisations. Information-security risk assessments (ISRAs) enable organisations to identify their key information assets and risks in order to develop effective and economically-viable control strategies (Baskerville, 1991; Roper, 1999; Peltier, 2001; den Braber et al, 2007). Various popular ISRA methodologies are used in industry, including methodologies such as OCTAVE, CRAMM, NIST SP800-30 and the AS/NZS 4360 standard (Alberts & Dorofee, 2004; Yazar, 2002; Stoneburner et al, 2002; AS/NZS, 1999). These ISRA methodologies ensure that critical assets are identified through a rigorous process involving different stakeholders, including senior management, operational managers and technical staff (Alberts & Dorofee, 2004). This facilitates protective action for assets considered valuable while also ensuring that resources are not wasted on protecting lesser risks or unimportant assets (Visintine, 2003). In other words, these risk assessments tend to be *asset-focussed* in that they are based on identifying information as points of value that are threatened, have vulnerabilities and require protection (Shedden et al, 2006).

Distinct from the discourse on information security, the literature on knowledge management has emphasised the strategic value of tacit and explicit organisational knowledge. Organisational knowledge is seen as having an inherent competitive and commercial value, where the loss of such knowledge could affect a company's ability to operate in a normal manner (Alavi & Leidner, 2001; Davenport & Prusak, 1998; Hansen et al, 1999). Such loss could further harm employee morale, customer confidence or have a direct impact on competitive performance. Some commentators have suggested that the protection of knowledge has not received adequate attention in the organisational security arena, despite its criticality (Ruighaver & Maynard, 2003; Bloodgood & Salisbury, 2001; Gold et al, 2005; Holsapple & Jones, 2005).

In this paper we argue that the asset identification sub-processes of most existing information-security risk assessment methodologies are limited in that they do not adequately address knowledge which, as Davenport (1998) notes, is 'baked into' organisational processes. We highlight these limitations through an illustrative case study in which we apply a typical information-security risk assessment methodology, OCTAVE-S, to a core organisational process. We examine the deficiencies of security assessment in OCTAVE-S in terms of process knowledge and consider how a knowledge perspective could be incorporated in security-risk assessments in general. In our analysis and discussion of this illustrative case, we offer some insights into how a process-focussed knowledge perspective could be incorporated into risk assessment methodologies.

INFORMATION SECURITY RISK ASSESSMENT: THE ASSET FOCUS

An information-security risk assessment (ISRA) is a systematic method by which organisations can identify and protect information assets to achieve a desired level of security, thus minimising losses of tangible and intangible assets (Lichtenstein, 1996; Blakely et al, 2002). Risks to assets are identified in terms of confidentiality, integrity and availability. The criticality of each risk is rated according to potential impact and likelihood of occurrence. Risks to organisational assets are collated and then prioritised on the basis of criticality for further action. (Roper, 1999; Alberts & Dorofee, 2004). An inadequate risk assessment process, or the absence of one, could lead to disastrous consequences for organisations, such as a loss in reputation, legal issues or direct financial impact.

The typical information-security risk assessment process commonly includes the phases of context establishment, risk identification and risk analysis (Whitman & Mattord, 2005; Shedden et al, 2006; Dhillon, 2007). Each of these phases is usually made up of a number of activities and sub-processes. There exist a number of popular information-security risk assessment methodologies including FRAP, CRAMM, COBRA, OCTAVE, OCTAVE-S and CORAS in use in Europe, the US and Australasia (Peltier, 2001; Yazar, 2002; Alberts & Dorofee, 2004; den Braber, 2007; Dhillon, 2007). These methodologies are widely used by industry (West et al, 2002; Shedden et al, 2006). Though these risk-assessment methods range in their underlying activities, order and depth, they generally apply a methodology consistent with context establishment, risk identification and risk analysis.

Context establishment considers the organisation's industry, structure, current security status overall goals and long-term strategy, ensuring that the risk assessment process does not conflict with organisational goals. This allows for the scoping and focus of the rest of the risk assessment process for maximum effectiveness and to ensure that any risks inherent to the organisation's industry or line of business are identified. Activities that define the evaluation criteria for the assessment (eg., what constitutes a 'high' impact to 'reputation'?) are also performed at this stage (Alberts & Dorofee, 2004).

Risk identification concerns the systematic discovery and selection of the most critical assets and the identification of the threats and vulnerabilities of each critical information asset. *Information assets* are viewed often as the IT infrastructural or informational resources that are of value to the organisation, commonly split into different categories, including: data, hardware, systems and applications (Visintine, 2003; Alberts et al, 2003; AS/NZS, 2004). A *threat* is defined as a category of objects which may present some form of danger to the critical information asset (Whitman & Mattord, 2005). *Vulnerabilities* are those security 'holes' or weaknesses inherent in the system that may present an avenue of attack against the information asset (Otwell & Aldridge, 1988).

Risk analysis concerns the determination of the probability (chance of the threat event occurring) and impact (the cost of compromising the asset). This creates a priority order of risks and allows assessors to determine whether risk should be avoided, mitigated, transferred or accepted (Whitman & Mattord, 2005). Analysis and assessment of impact and probability can be performed through either quantitative or qualitative means, offering a range of metrics derived from mathematical equations and statistical modelling or qualitative indicators such as interviews and documentation (Alberts & Dorofee, 2004; Roper, 1999).

When considering current risk identification approaches, we can see that current ISRA methods are still driven by an asset focus, given that critical information assets form the basis of the assessment proper. It is the information assets themselves that are assessed for threats and vulnerabilities. We must also stress that there is a focus in current ISRA methods on technical assets, eg. hardware and software (Salmela, 2008) rather than the richer organisational elements of information systems that include people, knowledge and practice (Dhillon & Backhouse, 2001). While this view is still consistently applied across current ISRA methods, current research establishes that the current focus on technical assets considerably limits organisational risk assessment (Siponen, 2005; Spears, 2006).

ORGANISATIONAL KNOWLEDGE AND KNOWLEDGE PROTECTION

Organisational knowledge has long been recognised as a resource of strategic significance (eg. Davenport & Prusak) and the importance of knowledge management is now well established (Hansen et al., 1999; Zack, 1999). A detailed examination of knowledge management is beyond the scope of this paper; instead we will highlight some of its aspects that are pertinent in conceptualising knowledge protection. First, we draw on Davenport & Prusak's widely cited definition of knowledge, stating that knowledge is "a fluid mix of framed experience" and "often becomes embedded not only in documents or repositories, but also in organisational routines, practices and norms (Davenport & Prusak, 1999).

Behind this view is Polanyi's (1962) distinction between explicit knowledge (that which can be articulated and encoded) and tacit knowledge (that which remains in the 'minds of knowers'). Building on this distinction in his well-known SECI model, Nonaka (1994) describes four processes through which organisational knowledge is created via conversions between tacit and explicit knowledge: socialisation, externalisation, combination and internalisation. Socialisation is the process of sharing tacit knowledge (eg. via means apprenticeships). Externalisation involves the articulation of tacit knowledge into explicit knowledge (this corresponds to what some sources term codification). Combination is the process of converting explicit knowledge into sets of more complex explicit knowledge. Lastly, internalisation involves the process of converting explicit knowledge back into tacit knowledge.

While some have argued that knowledge is inherently personal and contextually-bound, others have explored the idea of knowledge as distributed phenomenon beyond the single individual human mind. In this regard, knowledge and knowing are seen as attributes of groups of individuals. The notion of communities of practice (Brown & Duguid, 1991) builds on the idea of knowledge as an attribute of a collective. Indeed, the theory of distributed cognition proposes that knowledge extends beyond the mind of an individual and includes interactions between people, material and environmental resources (Hutchins, 1991; Hollan et al, 2000). In this regard, individuals transfer some of the cognitive load onto the resources and environment, embedding information and knowledge in artefacts (eg. displays, notice boards, documents).

Despite the wide recognition of the value of knowledge to organisations, research into knowledge protection has been described as 'thin' (Gold et al, 2001). A possible reason for this is an inherent conflict between the premises of knowledge sharing (typically assumed in the knowledge management literature) and those of knowledge protection. On the one hand, knowledge sharing is viewed as a valuable activity that gives individuals access to knowledge that will assists in completing tasks (Alavi & Leidner, 1999; Fischer & Ostwald, 2001). On the other hand, from an information security standpoint, such sharing activities bring new risks of knowledge falling into the 'wrong minds' and providing a means to inflict harm on the organisation or on its customers and partners (Whitman & Mattord, 2005).

Some commentators have explored the possibility that current knowledge management philosophies are inherently insecure. The need for a supportive 'knowledge control' process has been outlined – ensuring that required knowledge processors and resources are available in sufficient quality and quantity, subject to security requirements (eg., by Holsapple & Jones, 2005). However, there are few suggestions in the literature as to how this could be accomplished. One of the few proposals, for example, is 'data sanitisation' of codified knowledge (Oliveira & Zaiane, 2003). Holsapple & Jones (2005) also argue that using security risk management standards may be an option and that access controls and monitoring facilities should also be provided. This would aim to limit availability of the knowledge and increase confidentiality from a security perspective. Bloodgood & Salisbury (2001) further discuss the merits of limiting access to knowledge and ensuring that there is no single point-of-failure (eg., no single employee knows all).

Gold et al (2001) have broadly suggested several means to protect knowledge, including asset-based ISRAs. However, asset-based risk assessment methods typically deal only with explicit knowledge (i.e., that which can be codified or articulated in documents, databases, etc). Yet, as argued above, not all knowledge can be rendered explicit, nor can explicit records of knowledge often be understood and applied without related tacit knowledge. Indeed, it has been argued that the two forms of knowledge are 'mutually constituted' (Tsoukas, 2004) and explicit encodings must be actively re-contextualised on application.

In summary, it appears that is not sufficient to augment current ISRA methodologies merely by including the identification of ‘knowledge assets’ in the form of databases, or even key people. Indeed, a complex organisational process tends to rely on both explicit and tacit knowledge of various individuals and networks of experts. Therefore, understanding the full spectrum of risks associated with a particular process extends considerably beyond individuals and information assets alone. This line of thought suggests that if we wish to consider knowledge as a possible source of risk, the asset-based risk identification approach is likely to be insufficient.

ISSUES IN ASSET IDENTIFICATION: AN ILLUSTRATIVE CASE STUDY

In this section, we present a case study that illustrates typical shortcomings in information-security risk assessment methodologies regarding identification of assets in the knowledge space as opposed to the information space. In this case study, we have applied an information-security risk assessment methodology in a traditional sense to achieve typical results (including critical information assets). However, we also captured – through the use of narrative and a qualitative analysis based on interviews – critical process knowledge that was not explicitly discovered by the methodology.

Methodology

We adopted the case study approach to investigate a common ISRA methodology’s asset identification method and results. The approach of applying a risk assessment method in an organisation allowed us to determine precisely what assets were identified and evaluate the shortcomings of a typical method that operated using the common process outlined above. The application of case study research to this phenomena is appropriate in new topic areas such as this (Eisenhardt, 1989) as it is a research strategy that allows for an in-depth exploration in a particular context (here, a small, information-intensive, organisation) (Benbasat et al, 1987; Yin, 2003). SoftCo (a pseudonym) was selected for study as a typical example of an organisation that (a) has the need for ISRA because security concerns could have a severe impact, and (b) offers a sufficiently complex yet manageable research scope.

OCTAVE-S was selected as an ISRA methodology for study. Developed by Carnegie Mellon University and applied throughout industry, OCTAVE-S is a variant of the OCTAVE (Operationally Critical Threat and Vulnerability Evaluation) method, geared specifically for small-medium enterprises. Consistent with our literature review, the OCTAVE-S risk assessment model flows through the three phases of context establishment, risk identification and a risk evaluation coupled with an analysis of the desired risk treatment plans (Alberts et al, 2003). OCTAVE, applied notably in the healthcare industry and the US military (West et al, 2002), is representative of ISRAs used by industry more generally.

Data was collected from the security managers of the organisation using a workshop approach consistent with the OCTAVE-S methodology. The participants for these workshops were the security managers for the firm, described here as the ‘Security Head’ and the ‘Co-Security Manager’. The Security Head is a team leader of the Managed Services division which maintains the infrastructure and environment. He subsequently holds in-depth knowledge of SoftCo’s systems, security awareness and culture of the organisation. The Co-Security Manager is a systems administrator and supports the Security Head. These participants were selected due to their involvement in the area of study and because they provided different levels of domain knowledge and input based on the requirements of the OCTAVE-S methodology. For the purposes of this study, we focused upon a core business process for the assessment. The backup process was selected as it is common in organisations and is an extremely important security process designed to ensure that losses of data and hardware can be recovered (Stair & Reynolds, 1999). The workshops consisted of the participants answering structured questions and filling forms as per the OCTAVE-S method. Interviews were recorded and transcribed. A follow-up interview with the participants was conducted after the OCTAVE-S results were analysed in order to further explore points of interest and participant knowledge.

The SoftCo Case Study

SoftCo is an Australian software house and service provider employing 60 people and providing business-to-business e-commerce solutions for other, larger firms. These customer firms integrate their back-end systems with SoftCo’s such that purchasers sending their orders and invoices to suppliers will firstly route their files through SoftCo’s ‘Production Environment’. SoftCo then translates the documents or messages into formats readable by the other party’s systems. Therefore, SoftCo provide ‘middleware’ services and infrastructure for other organisations to send and receive purchase orders and other documents, with SoftCo translating these orders and documents into the customer organisations’ systems. Much of SoftCo’s IT infrastructure and computing systems are held off-site at a remote data centre. Of particular note is that the ‘translation maps’, or those files that perform these conversions of the order forms from one organisation into a format readable by the intended receiving organisation. These translation maps are the core of SoftCo, described as 'irreplaceable'.

SoftCo's backup process is vital as it stores copies of data and information critical to the core business processes of the organisation. If SoftCo's information systems and processes were to fail, the backup process would have retained and safely stored information and applications to restore operations. SoftCo's backup process is entirely automated, barring a few exceptions. Scripts initially coded and then "tweaked" (i.e., polished and refined) over time by the Security Head push data from the live Production Environment to the off-site backup server. The backed up data (including historical backups going back to the founding of the organisation) is held in the backup server. The backed up data is of high value given with the frequency with which problems occur with SoftCo data that requires restoring from the backups. The backups from the Production Environment are of every document that has passed through their system.

Case Study Results: Asset Identification

The OCTAVE-S assessment identified five critical information infrastructure assets for SoftCo's backup process, including three data assets, a personnel asset and an application asset. The results of the asset identification process are summarised in Table 1.

Asset Category	Asset Identified	Description
Data	Production data	The data that passes through the live Production Environment, including scripts, spreadsheets and directory structures. This is the data to be backed up.
	Backup files – Translation maps	The backed up translation maps (text-based scripts that 'translate' the contents of invoices and order forms into a format readable by the customer organisation's partner company). Stored off-site at a remotely-managed data centre.
	Backup files – Live data	The backup files of the data that flows through the Production Environment. Includes order forms, invoices, SQL database backups, scripts and e-mails. Stored off-site at a remotely-managed data centre.
People	Security Head and Co-Security Manager	The information security managers of the organisation. If they are not on-hand, the backup process will fail.
Applications	Backup scripts	The backup scripts are proprietary software that points the data from the live Production Environment to the backup storage locations.

Table 1. Critical Asset Identification Results

These assets satisfy the OCTAVE-S requirements for asset identification and critical asset selection, and are a common series of results from typical asset identification processes.

Case Study Results: Critical Process Knowledge Identification

The OCTAVE-S asset identification process suffered from the problem examined previously in that it did not identify a crucial area of vulnerability, which is knowledge about the backup process. Though questions were asked by the method on what knowledge a person might have ('what special skills or knowledge are provided by this person?'), it serves as a justification for the person to be considered a critical asset. The knowledge itself is not the target of an asset identification process nor does it surface any information about what those people know. For SoftCo, the security managers were identified as being information assets whose availability needed to be preserved. However, after analysis of the workshop transcriptions and follow-up interviews, a deeper understanding of the backup process and its key assets emerged related specifically to the key knowledge required in order to keep the process operational. It became apparent that while OCTAVE-S did identify the higher-level information assets critical to the ongoing operations of the backup process, it did not identify process knowledge. Key individuals were identified and described by the methodology, but not the richness and variety of their knowledge, including that which is tacit and explicit, and also the security managers' network of knowledge. If this knowledge was lost or not on hand for application, the process would fail with the potential for a 'catastrophic' (as reported by the participants) failure of the backup process.

Key Individuals

OCTAVE-S identified key personnel as part of its information asset identification process. As has been described, the security managers (who we refer to as their job titles Security Head and Co-Security Manager) are responsible for the monitoring and maintenance of the backup process to ensure its continued operation. Despite extensive automation of the process through the backup scripts, the security managers' interventions were still required. The Security Head outlined that their maintenance of the process was important.

Specifically, the application of OCTAVE-S enabled the risk-evaluation team to identify that the security managers were essential for the process. Otherwise the backup process itself would fail. Again reported by the Security Head:

> *If we weren't here, the backups would continue to function and everything would continue to work – if nothing stopped – it would run for about three weeks, and then stop because the server we back up to fails. It will get full. So there's some things where we actually manually go in and delete because you're not prepared to trust another process to automatically delete them.*

OCTAVE-S identified that in order for the backup process to remain in operation, the availability of the security managers would need to be preserved. The security managers would need to be in contact with and remain in control of the process through monitoring its functions, which they currently do through the use of e-mail and mobile phone alerts. Additionally, they have enacted an informal mechanism of staggering leave and absences.

Distributed Knowledge (Held Collectively)

However, OCTAVE-S did not consider that knowledge is not only held independently but shared between a work team following the theory of distributed cognition. The security managers do not work as individuals with this process: rather, they exist in a partnership, sharing knowledge and expertise. For example, when we asked about their documentation practices, the Security Head responded:

> *Yeah, very little documentation – I set up a lot of it, [the Co-Security Manager] maintains it and sets up stuff now. I trained [the Co-Security Manager] into it and he's worked it out and so it's pretty much the result of both of our thinking.*

This actually states that they have applied mutual thought, knowledge and expertise to the process. While either manager independently is important for the backup process, the current methods and operations are a product of both of their minds. Therefore, their distributed knowledge is just as important as the individually-held knowledge of each manager.

Individually-Held Tacit Knowledge

As individuals, the security managers have knowledge that is very difficult to articulate. They have built the process and its components through incremental customisation of the backup scripts over the course of many years. When discussing the nature of the backup process itself, the Security Head outlined that while it would be possible to document some elements of the process, it would not be possible to capture everything due to its 'messy' complexity:

> *Either one of us is critical. But if both of us weren't here, it would be difficult for someone else to come in and work out what we're doing, because it's so scripted and script-based and this process interacts with that process, so it's almost like spaghetti, to a degree. I mean it's very robust spaghetti, but if you had to flow-chart it all out, it would be a very messy flowchart.*

This is further reinforced by the Co-Security Manager's comments on their attempts at documentation and capturing their knowledge in codified form. When discussing how much could actually be clearly articulated into procedures, the Co-Security Manager explained that documentation could cover the general perspective, as he explained:

> *You still need to apply a level of understanding of the environment to understand how it works before; documentation will only tell you, like… There's only so much you can do, maybe 70% of it but then you need the experience outside of it to understand how it works.*

The additional 30% comes from their own experience and would be difficult to articulate. Though this is a routine process, the participants surprisingly reported that the adhoc nature of this process' development and the organic organisational environment it resided in left a number of tacit subtleties that would be difficult to articulate clearly or describe.

Therefore, there exists a great deal of tacit knowledge within the backup process that relates to an understanding of its complexities and how it actually operates. OCTAVE-S does not capture this tacit component.

Consequently, methods to increase availability of this knowledge (to prevent process failure) are not suggested by the methodology either.

Individually-Held Explicit Knowledge

Despite the tacit nature of much of the critical process knowledge, the security managers also expressed their desire to attempt codification of explicit knowledge and the importance of doing so. For example, the Security Head discussed the explicit knowledge of the backup process held by members of the organisation that have left.

> *... so very little of it was ever written down, [because] there was no need to formalise it because you knew what everybody was doing anyway. Then someone would leave and they'd take all that, what should have been written down and documented away with them. Less of a problem now because documentation actually takes place because the lines of communications are poorer, so it has to be documented for people to know what's going on, if you get what I mean…*

As the Security Head explained, individuals retain key explicit knowledge. This explicit knowledge can and should be codified to ensure the ongoing availability of critical process knowledge and subsequently the operation of the backup process.

As has been demonstrated SoftCo's backup system is complex, built upon backup scripts that have been extensively altered and customised over a long period. However, while OCTAVE-S identified the security managers as critical information assets, it is actually their knowledge and their network of knowledge that should be considered key. While the managers hold individual knowledge, they actually operate within a network, where various aspects of the backup process are, as stated by Security Head '*a product of both our thinking*'. However, their individual knowledge is also of critical importance, including that knowledge which is tacit and difficult to qualify and explain ('*it would be a very messy flowchart*') and that knowledge which is explicit and can be codified ('*it has to be documented for people to know what's going on*').

OCTAVE-S's method of identifying people as assets is adequate for a higher level view ('key individuals'), we argue that assessment methods must move beyond the individual. Such methods identify people as assets and it is their availability to the organisation that must be protected. However, we argue that while people themselves are important, it is also their individually-held and collective knowledge that must be identified for a risk assessment.

DISCUSSION

The case study illustrates the merits of following a structured ISRA to identify relevant assets that are critical to organisations. The OCTAVE-S methodology applied in the case pinpointed critical information assets such as the production data, backup files and backup scripts. Importantly, the methodology also identified two key people 'assets' – the Security Head and Co-Security Manager. Yet, as the additional case analysis illustrates, the current logic underpinning most of the current asset-based methodologies also misses key areas of vulnerability; in particular, individuals' knowledge of the backup process. The reason for this, we argue, is the rather simplistic focus on *assets* per se, and especially tangible assets (including 'people') that underpin current ISRAs.

We believe this to be an area that warrants further research, and in this section we explore how future ISRAs could incorporate a knowledge perspective. For this to occur we argue (1) it is necessary to adopt a process focus in ISRAs, and then (2) to consider process knowledge as part of the overall information security risk assessment. In terms of (1), we put forward propositions to guide future investigations of the comparative benefits of process versus asset-based ISRAs (cf. Dubin, 1969; Whetten, 1989).

Focusing on Processes in Information Security Risk Assessment

While the case study and analysis revealed knowledge as a key area of vulnerability, this only emerged when focusing on an organisational process. Without this perspective, it would be quite difficult to assess how 'valuable' an individual's knowledge is in terms of security risk assessment. This follows theorising in the knowledge management literature that sees knowledge when detached from its context as meaningless (cf., Thompson & Walsham, 2004). Though Australian security risk management guidelines and handbooks do suggest that knowledge should be identified as an extension of a 'staff' or 'people' asset category, this view is not uniform across ISRA methods or organisational implementations of these methods (AS/NZS, 2004; Shedden, 2005; DSD, 2007). It is only by adopting a process focus that knowledge assessed and vulnerability considered from a security risk mitigation perspective. Similarly, there could be other areas of vulnerability that asset based information security assessments could miss. In more general terms, this can be expressed as follows:

> Proposition 1: Process-based approaches to identifying information security risks yield areas of critical vulnerability that asset-based approaches fail to identify.

We have argued above that a process-focus is potentially valuable in security risk assessment. At the same time there are many business processes in organisations, some of which are core or mission-critical to the firm, and others which can be considered as ancillary. The same can be said about organisational assets; not all assets pertain to mission critical activities. ISRA methodologies that specifically focus on *core* processes are thus better suited to identify and elevate security risks that can have a significant impact on the organisation. Hence:

> Proposition 2: Information security risk approaches that focus on core business processes will tend to identify more mission-critical risks than asset-based approaches.

Incorporating a Process Knowledge Perspective in Information Security Risk Assessment

In the area of information security, organisation knowledge is an irreducible source of risk which is obscured in asset-based methodological approaches. ISRA methods such as OCTAVE-S describe that 'people' are a category of asset. As has been described, that person's skills and knowledge are described as attributes. However, their treatment of that category and the recognition of its importance by organisations is limited, as has been found here. As the case demonstrates, the security managers hold knowledge critical for the ongoing function of the backup process. From a knowledge perspective, the key vulnerability is not merely the availability of these individuals but their skills and knowledge (much of which is tacit). How then could ISRAs be augmented in order to identify critical knowledge?

In the propositions above, we have articulated that a process-based approach towards security risk assessment will add precision when considering what knowledge is indeed critical for a particular process. This is consistent with the notion that knowledge is 'baked into' business processes (Davenport & Prusak, 1998). Furthermore, in the subsequent case analysis we employed constructs from the knowledge literature that take into account the nature of knowledge and knowledge sharing. In combination this suggests mechanisms to incorporate a knowledge perspective in ISRA (see Figure 1).

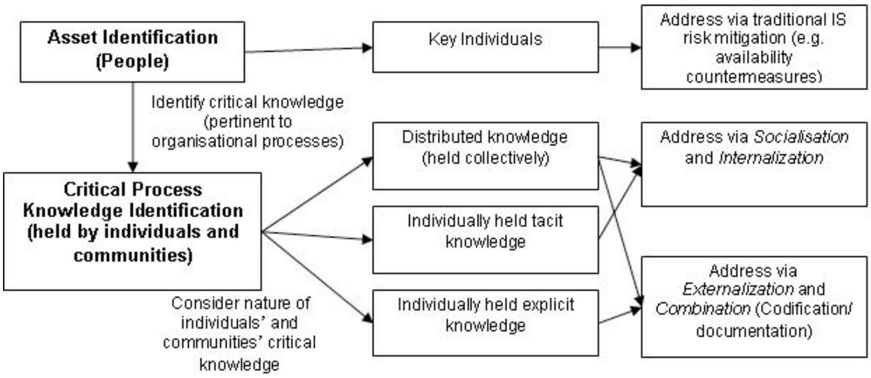
Asset Identification (People)
Key Individuals
Address via traditional IS risk mitigation (e.g. availability countermeasures)
Identify critical knowledge (pertinent to organisational processes)
Critical Process Knowledge Identification (held by individuals and communities)
Distributed knowledge (held collectively)
Individually held tacit knowledge
Individually held explicit knowledge
Address via *Socialisation* and *Internalization*
Address via *Externalization* and *Combination* (Codification/ documentation)
Consider nature of individuals' and communities' critical knowledge

Figure 1: Incorporating a knowledge perspective in information-security risk assessment

Moving beyond the identification of key people and traditional information security risk mitigation (the asset based approach), an augmented methodology should identify critical knowledge that is pertinent to typically core or at least critical organisational processes. In this regard, tacit/explicit individual knowledge and distributed knowledge that is pertinent to the process should be identified. In the case study, the two managers could be considered as a small community of practice. As with asset-based approaches, risk mitigation strategies for critical knowledge should form part of a knowledge-sensitive risk assessment. This would include strategies such as socialisation and internalisation (cf. Nonaka, 1994), which is the basis by which a degree of tacit knowledge could be shared. For example, having an apprentice 'shadowing' the key managers could be one strategy to spread the intimate knowledge they possess of the backup process to more people. Explicit knowledge relating to the process should also be considered. In this regard, strategies such as documentation and systemisation could be appropriate mitigation mechanisms to codify and combine explicit knowledge about the process. This would make it easier for a newcomer to gain insight about the backup process. Indeed, documentation of the backup process, at least those aspects which could be articulated explicitly, should be available from a quality assurance and general risk management perspective.

It should, however, be recognised that tacit and explicit knowledge are not easily separated. To codify the knowledge of the backup process into procedures or documents leads to a '*very messy flowchart*'. Given the managers tacit knowledge, an outsider to this process would still find it difficult to know when and why to follow the said procedures and when interventions in the automated process would be necessary. This underpins the need for a holistic knowledge perspective as part of an overall ISRA.

A combined information security and knowledge perspective would identify that knowledge of SoftCo's backup process (and the organisation's systems and security) is concentrated into only two minds (ie. too few people know too much). Few asset-based ISRA methodologies would identify this as a key vulnerability. If either of these employees grew disgruntled with their organisation, retired, or resigned, this would amount to a major threat for SoftCo's systems and processes generally, including the backup process. A combined perspective on this problem would facilitate action to control this risk. This may include tradeoffs between increasing the availability of knowledge (through knowledge sharing and externalisation, on a 'need-to-know' basis) cognisant of the risk of confidentiality breaches.

In summary, we suggest that a knowledge perspective could, and should, be incorporated into ISRAs. We believe the identification of core knowledge can occur through a business process-based focus. As illustrated by our second analysis of the case study, this can occur through conducting qualitative interviews with relevant staff members in the context of key business processes. Tools such as business processes mapping and rich process descriptions could further help to facilitate the identification of core knowledge and key knowledge workers. Such a more inclusive approach to security risk assessment would thus help to identify what knowledge is drawn upon in the process and what knowledge needs to be protected to control operations.

CONCLUSION

Information-security risk assessments (ISRAs) are important for organisations as they are the means by which critical information assets are identified, their threats and vulnerabilities assessed and a level of risk assigned and prioritised for future action. ISRA methodologies, however, mostly adopt an asset-based focus. By means of an illustrative case study, we have demonstrated the inherent limitations of a typical risk assessment methodology by exploring what it misses: critical knowledge of staff in the context of a complex but important organisational process.

To address such shortcomings in ISRAs, we argue for a focus on organisational processes and the inclusion of a knowledge perspective as a more encompassing approach for organisations to assess their overall security risk. Existing methods identify key individuals as 'critical information assets'. However, we argue that the individual's knowledge is of critical importance, as well as that knowledge which is distributed among a team or held collectively. We propose that protective techniques, for example the codification of explicit knowledge, or purposeful knowledge-redundancy and succession planning for tacit knowledge should be considered as part of the remedial action to protect critical organisational knowledge in a systematic and transparent manner.

We have illustrated that current ISRA methods do not identify security risks associated with knowledge in organisations. This implies that the unauthorised disclosure, modification and interruption or destruction of critical knowledge does not figure in the practice of security risk assessments. Although this paper has focused on availability of knowledge assets, further research must be conducted on the confidentiality and integrity of knowledge in security risk assessment methodologies.

REFERENCES

Alberts, C. and Dorofee, A. (2004). Managing Information Security Risks. Pittsburgh, Mellon Software Engineering Institute.

Alberts, C., Dorofee, A., Stevens, J. and Woody, C. (2003). Introduction to the OCTAVE Approach. Pittsburgh, Carnegie Mellon Software Engineering Institute.

Alavi, M. and Leidner, D. E. (1999). "Knowledge Management Systems: Issues, Challenges and Benefits." Communications of the Association for Information Systems (1:7).

Alavi, M. and Leidner, D. E. (2001). "Knowledge management and knowledge management systems: Conceptual foundations and research issues." MIS Quarterly (25:1), pp. 107-136.

AS/NZS (2004). Information Security Risk Management Guidelines. Sydney, Australia/ Wellington, New Zealand, Standards Australia/ Standards New Zealand.

Baskerville, R. L. (1991a). "Risk analysis: an interpretive feasibility tool in justifying information systems security." European Journal of Information Systems (1:2): 121-130.

Benbasat, I., Goldstein, D. K. and Mead, M. (1987). "The case research strategy in studies of information systems." MIS Quarterly (11:3), pp. 369-386.

Blakely, B., McDermott, E. and Greer, D. (2002). “Information Security is Information Risk Management.” NSFW '01, Clourcroft, New Mexico, USA.

Bloodgood, J. M. and Salisbury, W. D. (2001). "Understanding the influence of organizational change management strategies on information technology and knowledge management strategies." Decision Support Systems (31:1), pp. 55-69.

Brown, J. S. and Duguid, P. (1991). "Organizational learning and communities of practice: toward a unified view of working, learning and innovation." *Organization Science* (2:1), pp. 40-57.

Davenport, T. H. and L. Prusak (1998). *Working knowledge: how organizations manage what they know*. Boston, Massachusetts, Harvard Business School Press.

den Braber, F., Hogganvik, I., Lund, S., Stolen, K. and Vrallsen, F. (2007) “Model-based security analysis in seven steps – a guided tour to the CORAS method.” *BT Technology Journal* (25:1), pp.101-117.

Dhillon, G. and J. Backhouse (2001). "Current directions in IS security research: towards soci-organizational perspectives." Information Systems Journal **11**(2): 127-153.

Dhillon, G. (2007). Principles of Information Systems Security: Text and Cases. Hoboken, NJ, John Wiley & Sons, Inc.Dubin, R. (1969). Theory building. New York, Free Press.

DSD. (2007). Australian Communications-Electronic Security Instruction 33 (ACSI 33) Handbook 3, RISK MANAGEMENT.

Eisenhardt, K. M. (1989). "Building Theories from Case Study Research." *The Academy of Management Review* (14:4), pp. 532-550.

Fischer, G. and Ostwald J. (2001). "Knowledge Management: Problems, Promises, Realities, and Changes." *IEEE Intelligent Systems* January/ February 2001, pp. 60-72.

Gold, A. H., Malhotra, A. and Segars, A.H. (2001). "Knowledge Management: An Organizational Capabilities Perspective." *Journal of Management Information Systems* (18:1), pp. 185-214.

Grover, V. and Davenport, T.H. (2001). "General perspectives on knowledge management: Fostering a research agenda." *Journal of Management of Information Systems* (18:1), pp. 5-21.

Halliday, S., Badenhorst, K. and von Solms, R. (1996). "A business approach to effective information technology risk analysis and management." *Information Management & Computer Security* (4:1), pp. 19-31.

Hansen, M. T., Nohria, N. and Tierney, T. (1999). “What's your strategy for managing knowledge?” *Harvard Business Review* (March-April), pp. 106-116.

Hollan, J., Hutchins, E. and Kirsh, D. (2000). "Distributed Cognition: Toward a New Foundation for Human-Computer Interaction Research." *ACM Transactions on Computer-Human Interaction* (7:2), pp. 174-196.

Holsapple, C. and Jones, K. (2005). "Exploring Secondary Activities of the Knowledge Chain." *Knowledge and Process Management* (12:1), pp. 3-31.

Hutchins, E. (1991). Chapter 13: The Social Organization of Distributed Cognition. *Perspectives on Socially Shared Cognition*. L. B. Resnick, Levine, John M. and Teasley, Stephanie D. Washington, DC, American Psychological Association, pp. 283 - 307.

Lichtenstein, S. (1996). "Factors in the selection of a risk assessment method." Information Management & Computer Security **4**(4): 20-25.

Maynard, S. and Ruighaver, A.B. (2003). *Development and Evaluation of Information System Security Policies. Information Systems: The Challenges of Theory and Practice*. M. G. Hunter and K. K. Dhanda. Las Vegas, The Information Institute.

Nonaka, I. (1994). "A dynamic theory of organizational knowledge creation." *Organization Science* (5:1), pp. 14-37.

Oliveira, S.R.M. and Zaiane, O.R. (2003). “Protecting Sensitive Knowledge by Data Sanitization”. *Third IEEE Conference on Data Mining*.

Otwell, K. and Aldridge, B. (1988). “The Role of Vulnerability in Risk Management.” *1988 Computer Security Risk Management Model Builders Workshop*.

Peltier, T.R. (2001). *Information Security Risk Analysis*. Boca Raton, Auerbach.

Polanyi, M. (1962) *Personal Knowledge in M.Polanyi and H.Prosch*, Meaning. Chicago: University of Chicago Press

Roper, C.A. (1999). *Risk management for security professionals*, Butterworth-Heinemann.

Salmela, H. (2008). "Analysing business process losses caused by information systems risk: a business process anlaysis approach." Journal of Information Technology **23**(3): 185-202.

Shedden, P. (2005). Security Risk Management in Organisations. Department of Information Systems. Melbourne, University of Melbourne.

Shedden, P., T. Ruighaver, A.B and Ahmad, A. (2006). "Risk Management Standards - the Perception of Ease of Use". *The 5th Security Conference*, Las Vegas, Nevada, USA.

Spears, J. (2006). A Holistic Risk Analysis Method for Identifying Information Security Risks. Security Management, Integrity, and Internal Control in Information Systems. Boston, Springer Boston. 193/2006, pp.185-202.

Siponen, M. T. (2005b). "An analysis of the traditional IS security approaches: implications for research and practice." European Journal of Information Systems (14), pp.303-315.

Stair, R. M. and Reynolds, G. W. (1999). *Principles of Information Systems*. Cambridge, MA, Course Technology.

Stoneburner, G., Goguen, A. and Feringa, A. (2002). *Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology.

Thompson, M.P.A. and Walsham, G. (2004). "Placing Knowledge Management in Context." *Journal of Management Studies* (41:5), pp. 725 - 747.

Tsoukas, H. (2004). *Complex Knowledge: Studies in Organizational Epistemology*. Oxford: Oxford University Press.

Visintine, V. (2003). *An Introduction to Information Risk Assessment*, SANS Institute.

West, S., Crane. L.S. and Andres, A.D. (2002). *OCTAVE-DITSCAP Comparative Analysis*. Fort Detrick, Fredrick, U.S. Army Medical Research and Material Command.

Whetten, D.A. (1989). "What Constitutes a Theoretical Contribution?", *The Academy of Management Review*, (14:4), pp. 490-495.

Whitman, M. E. and Mattord, H. J. (2005). *Principles of Information Security*, Thomson Course Technology.

Yazar, Z. (2002). *A qualitative risk analysis and management tool - CRAMM*, SANS Institute.

Yin, R. (2003). *Case Study Research, 3rd Edition*. Thousand Oaks, Sage Publications.

Zack, M. (1999) Developing a knowledge strategy. California Management Review, (41:3), pp. 108-145.

COPYRIGHT