2010

Information Security Risk Assessment: Towards a Business Practice Perspective

Piya Shedden
University of Melbourne

Wally Smith
University of Melbourne

Atif Ahmad
University of Melbourne

Originally published in the Proceedings of the 8th Australian Information Security Mangement Conference, Edith Cowan University, Perth Western Australia, 30th November 2010

Information Security Risk Assessment: Towards a Business Practice Perspective

Piya Shedden, Wally Smith and Atif Ahmad
Department of Information Systems
University of Melbourne
Victoria, Australia
psheddon@unimelb.edu.au
wsmith@unimelb.edu.au
atif@unimelb.edu.au

Abstract

Information security risk assessments (ISRAs) are of great importance for organisations. Current ISRA methods identify an organisation's security risks and provide a measured, analysed security risk profile of critical information assets in order to build plans to treat risk. However, despite prevalent use in organisations today, current methods adopt a limited view of information assets during risk identification. In the context of day-to-day activities, people copy, print and discuss information, leading to the 'leakage' of information assets. Employees will create and use unofficial assets as part of their day-to-day routines. Furthermore, employees will also possess important knowledge on how to perform their functions within a business process or information system. These are all elements of business 'practice', a perspective that would yield a richer and holistic understanding of an organisation's information assets and vulnerabilities. This perspective is not captured by traditional ISRA methods, leading to an incomplete view of an organisation's information systems and processes that could prove detrimental and damaging. This paper hence suggests that a business practice perspective be incorporated into ISRA methods in order to identify information leakage, unofficial, critical information assets and critical process knowledge of organisations.

Keywords

Information security risk management, asset identification, knowledge security, information leakage, business practice.

INTRODUCTION

The security of this information is of paramount importance and a critical area of information systems (IS) study and application. (Gerber & von Solms, 2005). Security incidents can present substantial losses to industry through the direct loss of information assets, a loss in organisational reputation and customer confidence, a loss of employee productivity or the risk of legal issues (Alberts & Dorofee, 2004).

Information security risk assessment (ISRA) methodologies are the primary means by which organisations achieve an ideal level of information security in an economically viable manner (Baskerville, 1991a; Dhillon & Backhouse, 2001; Siponen, 2005; Whitman & Mattord, 2005). ISRA methods such as OCTAVE, FRAP, CORAS, CRAMM and the Australia HB231:2004 have been developed along with supporting tools and documentation that tailor security control implementations to organisations (Peltier, 2001; Stolen et al, 2002; Yazar, 2002; Alberts & Dorofee, 2004; AS/NZS, 2004; den Braber et al, 2007).

However, these methods have critical limitations in that they adopt a technical perspective. Though information assets (ie. 'anything of value' in an organisational information system) are the focus of an assessment, current ISRA methods do not consider 'unofficial' copies of assets, or such unofficial assets created or defined by individual users that are defined and established through business practice (Ahmad et al, 2005; Spears, 2006; Shedden et al, 2011). Furthermore, current methods do not appropriately consider people and their knowledge as assets of the organisation (Alberts & Dorofee, 2004). Instead, the focus is again on the technical elements of the system under review.

In this paper, we argue that current ISRA methodologies must incorporate a business 'practice' perspective into the identification of information security assets. The paper will outline the traditional perspectives of current ISRA methods, describing phases of context establishment, risk identification and risk analysis, the importance of business process perspectives in security and the nature of business practice. This paper will ultimately present the importance of a practice perspective to ISRAs, suggesting a future research agenda.

THE TRADITIONAL ISRA AND ASSET IDENTIFICATION PERSPECTIVE

Information security risk assessment (ISRA) methodologies are the means by which organisations attempt to identify and protect information assets to achieve a desired level of security in order to minimise tangible and intangible losses (Blakely et al, 2002; Reid & Floyd, 2001; Eloff & Eloff, 2005). Through following the phases of traditional ISRM methodologies, organisations attempt to achieve a cost-effective definition of its desired level of organisational information security and contribute to overall organisational improvement (AS/NZS, 2004).

The Purpose and Importance of Traditional ISRA Methods

Traditional ISRA processes are the means for identifying an organisation's desired security level (Whitman & Mattord, 2005), forming the basis of any well-protected, secure information system (Kokolakis et al, 2000; Siegel et al, 2002). Current methods attempt to provide order to the ways in which an organisation determines what controls to implement in order to mitigate or reduce security risks (Baskerville, 1991b). It is through this process that organisations will identify those assets critical for an organisation's operations and survival, the threats to each asset's confidentiality, integrity and availability, its vulnerabilities and then quantify them in terms of consequence and likelihood to produce an accurate, prioritised list of risks for further action (Roper, 1999; Alberts & Dorofee, 2004). The organisation must then consider how the prioritised risks can be controlled through selection of one of four basic control strategies (avoidance, mitigation, transference or acceptance) that then outline how the organisation can best deal with the risk (Whitman & Mattord, 2005). The organisational environment after the implementation of these controls must be monitored, ensuring that the controls are maintained and the desired level of coverage is actually achieved (AS/NZS, 2004a).

A typical ISRA method is composed of three phases: context establishment, risk identification and risk analysis (Roper, 1999; AS/NZS, 2004; Dhillon, 2007; Shedden et al, 2006). The objective of these phases are to establish the organisational context, identify key organisational information assets, select a sub-list of critical information assets, identify asset threats and vulnerabilities and measure these threats in terms of their probability of occurrence and impact if the threat were to occur (Halliday et al, 1996; Lichtenstein, 1996; Roper, 1999; Whitman & Mattord, 2005). This information can subsequently be used to create risk treatment plans and justify the costs of control selection, development, installation and maintenance to management (Baskerville, 1991a).

The objective of organisational ISRM is to ensure that confidentiality, integrity and availability can be delivered for key organisational information assets, in a cost-effective manner (Slay & Koronios, 2006; Hamilton, 1999; Stacey & Helsley, 1996). It provides the information required in order to make accurate security planning decisions to reduce, mitigate, transfer or accept risks (Straub & Welke, 1998; Whitman & Mattord, 2005) in an economically balanced manner (Merkow & Breithaupt, 2006; Baskerville, 1991b). Through this justification, the ISRM process is subsequently an important means of ensuring senior management buy-in and support for the desired level of security in the organisation (Baskerville, 1991a).

The Asset Focus of Current ISRA Methods

ISRA methodologies currently maintain an asset focus during the identification of risk (Shedden et al, 2011). Information assets are the focus of assessments as they are the organisation's chief objects or items of value (Jones & Ashendon, 2005). Typically, information assets are considered to be the infrastructural and informational elements that comprise information systems, including hardware, software, people, data and information (Whitman & Mattord, 2005; Salmela, 2008). Throughout the course of the assessment, it will be these infrastructural information assets that are the unit of analysis: it is their risks will be identified and assessed, so that these objects of value can be secured against potential attack. It is therefore imperative that the correct information assets be identified and that organisations select their critical assets from a complete list. Otherwise, the wrong assets may be assessed for risk, or key information assets that are important for the organisation's operations may be hidden and remain unassessed.

EXPLORING PROCESS AND PRACTICE PERSPECTIVES IN ISRA

Despite their prevalent use throughout industry, traditional ISRA methods adopt a limited, technical approach to asset, threat and vulnerability identification. That is, they adopt the view that systems consist of hardware, software, information and data assets with IT department members typically considered responsible for conducting the assessment (Halliday et al, 1996; Kokolakis et al, 2000).

However, we argue that this current view of assets is limited. While information security was historically a physical, mechanical issue due to procedurally and physically separate batch processing facilities (Gerber & von Solms, 2005), information systems are now deeply embedded within a rich social environment, influenced by user behaviours and formal and informal work practices (Dhillon & Backhouse, 2001; Brown & Duguid, 2002; Spears, 2006). As such, there is subsequently an identified need to move towards a more socio-organisational view of security as a whole, away from the technical perspective that pervades current thought (Dhillon & Backhouse, 2001; Siponen, 2005; Shedden et al, 2009).

Information assets reside within this rich business environment, where information assets are not static. Rather, assets evolve and change, given that people use and create assets dynamically as part of their formal and informal work routines during the course of business processes (Farris, 1979; Brown & Duguid, 2002; Ahmad et al, 2005). A work environment is flexible and 'messy', where individuals pursue workaround activities and shortcuts based on their own initiative (Sasse & Flachais, 2005).

Such activities have an impact on the security risk profile of the organisation. Traditional ISRA methods form a largely 'static' and isolated view of information assets: the current technical focus considers assets as disparate objects, largely ignoring the social elements of information systems that are made up of people, processes, knowledge and informal practices and activities (Rohrig & Knorr, 2004; Ahmad et al, 2005; Spears, 2006). However, these social, practice-based elements are the source of significant risk. Individuals who create their own assets (eg. spreadsheets used for their own work tasks, incorporating financial data taken from a secure system), informal activities and the uncontrolled copy of information between digital, physical and knowledge 'containers' (Ahmad et al, 2005) present vulnerability issues for organisations.

Traditional methods also often produce high-level results, summarising information assets into 'buckets' or identifying information assets at a high level. While reducing workload, these actions run the risk of producing generic outcomes, often identifying threats and vulnerabilities at a system-level as opposed to the specific infrastructure, information and people that form that system (Shedden et al, 2006). A means of avoiding this issue is required, given that a deeper level of granularity in asset identification would facilitate the identification and treatment of risks specific to individual assets (Shedden, 2005).

We hence argue that the incorporation of a business *process* perspective into ISRA would provide organisations with a method to deal with these limitations of traditional ISRA methods. Security literature points to the need for the adoption of business process-based security methods in order to more holistically identify and analyse the security risks of the firm (Halliday et al, 1996; Kokolakis et al, 2000; Dhillon & Backhouse, 2001; Olson, 2005; Siponen, 2005; Spears, 2006; Salmela, 2008). Through a process perspective, organisations are able to 'frame' an assessment, identifying key information assets that support the business processes, which in turn support core business functions (Halliday et al, 1996). Traditional methodologies typically consider the IT infrastructure of an organisation (Spears, 2006). However, IT infrastructure is naturally used in support of business processes which deliver value for organisations. Adopting a process perspective would allow organisations to consider their most important business processes first, and considering the specific IT infrastructure that supports the processes. This would hence drive a more accurate and explicit understanding of the business impacts of an information asset's compromise (Salmela, 2008). There are current initiatives that do attempt to cover this business process approach to security.

BPM-ISRA Initiatives

Kokolakis et al (2000) suggests that organisations should look to the use of business process modelling (BPM) in order to establish this understanding of a process' security requirements, modelling tasks, actors and information flows. Methods such as POSeM (Rohrig, 2002; Rohrig & Knorr, 2004) and Tropos (Mouratidis et al, 2003) have understood that traditional checklist-based and ISRA methods offer a broad, generic and limited perspective, not effectively tying the assessment method to the business (Kokolakis et al, 2000). Process-level risk assessments allow organisations to better establish the business context by firstly determining what its important business functions are, the processes that support them and the IT infrastructure that in turn supports the processes (Halliday et al, 1996). Within this framework, BPM-ISRA methods understand that business processes are the means by which organisations create business value (Jones & Ashendon, 2005). The business process models are then developed to underline the security requirements and restrictions of each task, actor and workflow within the process. Using these models as the basis to establish security levels in organisations permit the implementation of security controls directly into the business process itself at the task level. The representation of workflows and activities through process models is also explored through other research paradigms: Siponen (2003) highlights the concept of information modelling, which expresses the security constraints of organisations as object-oriented or structural diagrams.

While the use of BPM enables organisations to determine information flows, work tasks, user assignment to tasks and security requirements of tasks, BPM-ISRA approaches still adopt a technical, positivist view of organisations much like the criticisms of the traditional ISRA perspective (Siponen, 2005). When examining current methods, BPM-ISRA methods focus again on outlining the technical security requirements of tasks and work activities without paying heed to social elements. That is, they still establish the 'formal' view of how organisations should operate without studying actual work practice. Furthermore, the majority of BPM-ISRA and information modelling methods are not focused on security from the information asset-threat-vulnerability ISRA perspective. Instead, BPM-ISRA and related initiatives concern the assessment of security requirements of business processes during the design and development stages of the process or information system. The perspective is therefore inconsistent with the shifting landscape of security and the ISRA paradigm, where assessments are periodically conducted on existing information systems to identify new or emerging risks to existing systems.

Limitations of BPM-ISRA

Consistent between the traditional and BPM-ISRA perspectives is the lack of a social understanding of the nature of information system practice involving the system's business context, IS practice and people. This view does not consider that the methods by which users conduct their work tasks using information systems can present a major source of risk to organisations. While BPM-ISRA methods attempt to establish the business context by modelling business processes (consistent with the hierarchy put forward by Halliday et al, 1996) and the security requirements of tasks and actors, they do so through a technical, mechanical perspective rather than through any examination of IS 'practice' (Brown & Duguid, 2002). What BPM-ISRA and traditional methods identify are 'static' and formal information assets. In traditional ISRA methods, information assets are not considered as part of a broader context, incorporated within business processes that directly create value for organisations. However, this process perspective again does not consider IS 'practice', involving people and how they create, store, manipulate and/ or delete information through informal, workaround activities (Ahmad et al, 2005).

Information Asset Identification and Analysis through the Practice Perspective

Current ISRA methods adopt a technical and mechanistic approach when identifying information assets. Spears (2006), Kokolakis (2000) and Halliday et al (1996) each highlight this focus on a technical view, not considering people and processes. Ahmad et al (2005) suggests that traditional methods do not appropriately take the context of the asset into consideration during the assessment: that is, how the asset is applied and used in the course of a business process which may be a source of risk. Existing ISRA approaches are focused on technical components and issues, whereas the focus should instead be "on the organisation's critical business processes" (Halliday et al, 1996). This focus on the technical leads to an incomplete assessment of the organisation's critical assets and their associated risks as it is not tied closely with the business environment (Kokolakis et al, 2000). Additionally, a focus on technical assets and not people or their knowledge ignores the fact that people and processes themselves are 'significant' sources of security risks (Spears, 2006).

A process perspective in ISRA is still limiting. The development of BPM-ISRA methods is an attempt to specify security requirements in a more business-focused manner (Rohring, 2002; Backes et al, 2003). Through the application of BPM, organisations can link its processes and output directly to security goals and controls (Rohring, 2002). However, BPM-ISRA methods are limited in that they are focused on a 'technical and mechanistic' view of organisational work (Siponen, 2005) and do not study the way in which individuals perform their work during the course of a business process, which is a source of risk (Ahmad et al, 2005; Spears, 2006). Methods such as MoSS and POSeM (Herrmann & Herrmann, 2006; Rohring, 2002; Rohrig & Knorr, 2004) are concerned with representing the official view of business processes and defining a formal workflow. While this is a useful in identifying the information assets actually used during the course of the business process (eg. identifying data sets, servers, etc), they do not examine asset leakage, workaround activities or other elements of IS practice.

Business Practice

Therefore, we argue that business *practice* is an ideal perspective through which to improve current information asset identification methods. Brown & Duguid (2002) suggest that the process-oriented view of business processes and information systems is linear, emphasising strict work activities that pass data and information from one activity or task to the next. However, the examination of work *practice* rather than process allows organisations to understand the informal activities involved in actually getting work done with human input and workaround procedures people perform. Therefore, a criticism of traditional and BPM-ISRA methodologies is that they ignore the nature of the 'informal'

organisation, or those activities and flows of information and knowledge that are not officially supported by, mapped, modelled or encouraged by the organisation (Farris, 1979).

The concept of business 'practice' is related to the informal organisation and to business processes. Business processes identify activities and tasks performed by actors in a procedural, formal manner placed upon actors by the formal organisation. Business practice is the study of how individuals go about their work in the informal organisation. Brown & Duguid (2002) outline that the process view of organisations are that "machines work quite predictably", following patterns and routines in a predictable manner. Process is essentially a mechanical view of organisational behaviour, operating as a machine would when properly programmed and executed. Human behaviour does not factor in - a process follows a series of steps and the social context is not taken into account.

However, the practice view of organisational activity consists of the methods by which individuals actually operate within the context of an organisational environment. This involves the collaboration between parties, storytelling and shared experiences and improvisation in the organisational environment (Brown & Duguid, 2002). Organisational practices concern user behaviour and their actions within business processes and activities.

From a security perspective, such actions may result in the unwitting leakage of information and the creation of information assets to support workaround activities. Also embedded in practice and in process is critical knowledge (Brown & Duguid, 2001; Hislop, 2009). Existing methodologies only capture the formal and technical view of an organisation's system or process. This 'informal' organisation refers to which reflects upon the "spontaneous efforts of individuals and subgroups", which may support or go against the organisation's formal processes and requirements (Farris, 1979). That is to say, ISRA methods are focused on capturing the mechanical, formal view of organisations and the scoped target for assessment. However, the nature of the informal organisation is a critical concept, offering a richer version of organisational life that goes beyond 'process'. The way in which work is performed within an organisation can have an impact on security risk (Ahmad et al, 2005). Such concepts as asset 'leakage' reflect upon the informal nature of organisational practice.

Information takes many forms in organisations and business processes, being "transmitted across networks, printed or written on paper and spoken in conversations" (Pipkin, 2000; Winkler, 1996). As such, ISRA methodologies only take into account an 'official', explicit view of information when evaluating asset threats and vulnerabilities. However, this is distinct from the view from within organisations where individuals will pursue informal activities and workarounds of their own accord in support of the formal process (Farris, 1979).

In this manner, information can change forms through workaround activities that involve printing documents, photocopying reports, saving work onto a laptop or copying files to a USB stick, also referred to as information asset 'leakage' (Ahmad et al, 2005). Furthermore, it is suggested that a practice perspective has the capacity to identify critical knowledge embedded in business processes and to identify information assets at deep levels of granularity.

Asset Leakage – Concept and Impact

Asset 'leakage' is the product of both employee negligence and 'broken' business processes, reflecting on individuals performing workaround activities away from the formal view of the organisation (Ponemon, 2006). A source of organisational vulnerabilities exists in an organisation's daily execution of activities (Yue et al, 2007). Traditional ISRA methodologies focus on identifying and assessing information assets residing within computer systems in storage or in transmission across a network (Whitman & Mattord, 2005). However, information in organisations exists in many different forms, including the physical, digital and in the minds of users (Ahmad et al, 2005). Confidential information can be stored on workstations and laptops, be printed onto paper, e-mailed to alternate addresses, faxed and spoken about in formal and casual meetings (Hill & Pemberton, 1995; Winkler, 1996).

Though not widely considered by organisational staff, the leakage of these information assets can occur through work practices: data can be easily removed from a secure environment to a relatively unsafe home office through UBS sticks, or printed and removed in folders or binders as illustrated in several studies (Jones, 2005; Ponemon, 2006). In a survey of large organisations, Ponemon (2006) outlines that 81% of respondents reported that a laptop was stolen or lost, often removed off-site and left in public spaces or taxi cabs; a significant risk given that individuals store confidential data on unencrypted hard drives. Jones (2005) conducted a study of second-hand hard drives, sold to the public by organisations. The author discovered that over half the disks "contained sufficient information from which the organisations could be identified", 51% contained personal information including addresses and contact numbers, and 20% contained financial information. When combined with other cases of leakage previously discussed (eg. the leak of 25 million Britons' personal information; Pfanner, 2007), the potential loss can be severe.

Identifying Asset Leakage in the Informal Organisation

During a business process, information assets are manipulated, stored, retrieved and/ or deleted from a system. Throughout processes, information asset can change between the digital, physical and knowledge containers or be copied within a container in unofficial activities and removed to a less secure location and/ or reside in the mind of an employee depending on the nature of the process and the official and unofficial activities performed by individuals (Ahmad et al, 2005). Figure 1 demonstrates this 'asset leakage'.

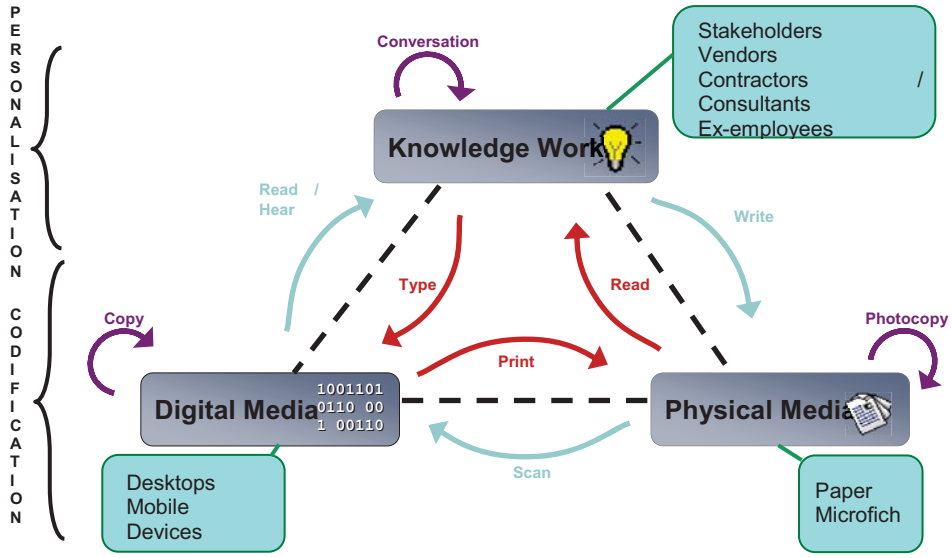

Figure 1 – information leakage in organisations (Ahmad et al, 2005)

Figure 1 illustrates that, in the context of a business process, information can exist in any one of these three forms. At any time, information assets can be copied between containers whilst still residing in the original format. Information can also be replicated within the same container, but stored elsewhere (eg. copying documents between an organisational workstation and a laptop).

This compounds the risks associated with the information asset beyond what a generic risk assessment model would detect (Ahmad et al, 2005). While some methods do identify the types of business process activities that occur within a targeted system (den Braber et al, 2007; Yazar, 2002), they are not geared towards identifying this 'leakage' from unofficial workaround activities. Existing security controls can cope with the official views of the digital and physical containers. However, these controls are negated if an individual were to copy work outside of the official, formal organisation environment to an unofficial container outside of the scope of current controls.

However, we suggest that a practice perspective to ISRA can identify asset leakage. Through the study of business processes, official information flows can be mapped to determine the formal state of the process flows as per BPM-ISRA. However, interviewing employees to outline how they actually perform tasks and whether information is leaked through their informal, unofficial activities and workarounds as is common (Sasse & Flachais, 2005; Bernard, 2007) could reveal actual work practices and the 'real' information flows distinct from official process maps. These flows could reveal the copying of information to personal PCs for work purposes, to USB memory sticks and the printing and photocopying of confidential information to aid work.

Asset Identification Granularity and Accuracy

When engaging traditional ISRA methodologies, organisations tend to default to an overly high-level unit of analysis when attempting to identify assets. Even with the use of ISRA methodologies, organisations often identify the information system itself as the information asset due to a number of perceptions that are distinct from reality, including

'ease of use' (Shedden et al, 2006). This leads to an incorrect and at best generic security outcome (Ahmad et al, 2005; Shedden, 2005; Shedden et al, 2006). That is, organisations will conduct an ISRA of a scoped information system as a 'black box' without considering its detailed information assets and their specific threats. This is due to inappropriate organisational application of the methodologies and as the methods themselves do not drill into a deep enough level of detail when identifying information assets (Lichtenstein, 1996; Shedden, 2005).

An organisation in these circumstances would be successful in identifying the higher-level, generic and broader risks to the system. However, those risks specific to a particular information asset (eg. individual servers, confidential data storage on workstations, applications, procedures, etc) – each possessing their own specific, personal threats, vulnerabilities and subsequent risk profile – would remain undiscovered. A case study of an Australian state government department revealed that the security staff themselves are unsure of whether they are identifying the correct assets and hence evaluating the proper risks to the firm (Shedden, 2005).

However, a business practice perspective can be used to facilitate in-depth asset identification. Specific exploration of what information assets are required to ensure the operation of key critical processes would identify a broad range of critical information assets. That is, the application of process perspectives to ISRA would yield a more complete register of information assets required for the operation of a process. However, the practice perspective could identify the assets actually used by individuals in their day-to-day activities. These may include user-created assets that are used in addition to or instead of the formal assets recognised by the organisation (Spears, 2006). We hence argue that an emphasis on the analysis and identification of assets in a business practice context should provide a deeper level of granularity. For instance, interviewing employees on their work practices and what they require to perform their activities would reveal what information assets are required for them to perform their tasks in particular processes.

The Security of Critical Knowledge

A business practice perspective would examine the important people and critical knowledge required for a given process to function, given that knowledge is embedded in organisational process and practice (Davenport & Prusak, 1998; Hislop, 2009). Though people are considered by most traditional ISRA methods as potential 'assets', they typically place little emphasis on their assessment beyond user identification and authentication (Spears, 2006). Methodologies such as OCTAVE, widely used in the US for hospitals and the military (West et al, 2002), adopts the view that while 'people' can be classified as information assets (as they are an integral part of an information system; Stair & Reynolds, 1999), organisations are encouraged to look to the systems and applications that those people use as critical information assets (Alberts & Dorofee, 2004).

However, knowledge is an integral part of organisations, embedded in organisational business processes and considered a significant driver of process efficiency, competitive advantage and accuracy in decision-making (Davenport et al, 1998; Zack, 1999; Schultze & Leidner, 2002). Knowledge is of high strategic importance (Scheepers et al, 2004) and is embedded in the social practice of information systems and not explicitly recognised or assessed by current ISRA methods as outlined.

Despite the importance of knowledge and the need for protection, there is little literature on knowledge and knowledge security (Gold et al, 2001; Shedden et al, 2009). Gold et al (2001) articulates that knowledge must be protected and broadly suggests several means, including information security risk assessments. Shedden et al (2009, 2011) presents a model for knowledge security, employing knowledge sharing practices such as externalisation and codification to ensure adequate availability of knowledge. ISRA methods do consider 'people' as information assets, as they form an integral part of an information system (Roper, 1999; Stair & Reynolds, 1999).

From an IS practice perspective, people may have knowledge critical to the operation of information assets or the business processes themselves. Case studies conducted at a software engineering firm have indicated that processes fail if knowledgeable staff are unavailable to apply that knowledge (Shedden et al, 2011). Alternatively, people may retain knowledge that should be considered confidential.

ISRA methodologies do not consider knowledge as a discrete 'asset' for protection, instead preferring to focus on technical assets (eg. OCTAVE electing to identify the systems a person uses over the person) as established. We have examined how traditional ISRA and BPM-ISRA methods are focused more on the mechanical or engineering-type view of representing or 'baking' security into organisations and their processes. However, the existence of a knowledge container and the input that people provide in a business presents further security concerns (Ahmad et al, 2005; Spears, 2006).

The concept of a 'person' as an asset is considered a technical limitation of ISRA methods. We have examined, for example, the OCTAVE methodology's treatment of people assets and have highlighted that the distinction is not made between protecting the person (and hence the operation of a system, or an application) and the person's knowledge (Alberts & Dorofee, 2004). Currently, methods such as OCTAVE outline that a person should be made available to the organisation if they are important or hold critical knowledge.

However, including knowledge in the scope of an ISRA would ensure that a source of critical competitive advantage would remain protected and available. Internalised information, as per the asset leakage issues discussed, could be controlled. Further, given that knowledge is embedded within process and practice, interviewing people on what knowledge is required to operate an asset and conduct an activity could lead to control strategies that share the knowledge to ensure ongoing operational and process efficiency (Shedden et al, 2009).

Therefore, application of a practice perspective to ISRA could incorporate a knowledge focus. Identifying critical operational or process knowledge through ISRAs could lead to greater availability of business processes and services. Rather than placing an emphasis on employee availability, treating their knowledge as the asset could lead to controls such as externalisation and codification of that knowledge (Shedden et al, 2009), hence distributing this critical knowledge to other parties. Conversely, if knowledge was identified as confidential, then restrictions through policy and training could be applied to ensure that the distribution of this knowledge is limited.

ISRA AND BUSINESS PRACTICE: TOWARDS A RESEARCH AGENDA

We suggest that if organisations were to study how business processes actually operate and how people actually perform their tasks and manipulate information, the risks, information and knowledge assets born from social interaction and unofficial activities could be identified. These elements of IS practice can introduce new risks and information assets into the organisation through informal workaround activities not captured by traditional ISRA methods. Current approaches to risk identification are based on technical and mechanical methodologies. They do not consider the vulnerabilities introduced by work activities in business processes. We understand that traditional ISRA methods adopt a technical focus to information assets, considering hardware, software, data and information. These methods adopt a narrow view of the importance and involvement of people and the influence of IS practice on an organisation's security profile. Current perspectives on risk largely ignore the business context of the target information systems. Traditional ISRA and BPM-ISRA approaches are incomplete. Neither consider that a major source of risk are the organisation's people and its own processes (Spears, 2006).

In particular, asset 'leakage' occurs during the context surrounding work performed in organisations and their business processes (Ahmad et al, 2005). Such leakage occurs through IS practice (Brown & Duguid, 2002), concerning those informal workaround activities that individuals perform to support their tasks. However, the identification of information asset leakage would result in a broader view of organisational information assets and therefore a more complete view of information security risks. Therefore, we propose that:

> **Proposition 1:** Asset leakage can be identified if a practice perspective is considered in ISRA, as the handling and treatment of information assets can be traced through analysis of dynamic work environments as opposed to a static perspective as is currently offered.

We have discussed the importance of critical knowledge within organisations and how knowledge must be identified and secured. Knowledge forms an important element of information systems and business processes (Brown & Duguid, 2002; Davenport & Prusak, 1998). However, knowledge security is a relatively unexplored area of research (Gold et al, 2001) and is not assessed through current ISRA methods. However, we have suggested that if organisations were to include knowledge as critical assets, not just 'people', a significant source of competitive advantage and a major driver of operational efficiency could be secured. We therefore propose the following:

> **Proposition 2:** Critical knowledge can be identified through a practice perspective, given that knowledge is critical for organisational operations and that it is embedded within business processes and activities.

Finally, a view of asset granularity and accuracy was presented. Organisations are currently identifying information assets at a high level, facilitated by current ISRA methods (Shedden, 2005). We suggest that a practice perspective could provide further insight into what information assets are currently used in critical business processes and what assets are critical for employee activities within each process. Adopting a practice perspective could lead to greater accuracy in asset identification if employees are questioned on what actual IT infrastructure and user-created assets are required for their work. Therefore, we propose the following for further study:

Proposition 3: Information assets can be identified at deeper levels of granularity through the application of a business practice approach.

If ISRA methods are geared towards the identification of information assets through a socio-organisational, practice-based approach, organisations would be better equipped to explore these issues. There is a 'growing disillusionment' with the formal and mechanical security analyses methods of information systems, given that the manner in which information systems 'dynamically interact' with their business context and users is not explicitly analysed (Dhillon & Backhouse, 2001). Therefore, there is the need to move towards a more holistic ISRA methodology that is able to identify the social context surrounding information systems for the purposes of identifying organisational information assets and security risks. Such perspectives will yield rich information to drive accurate security risk assessment beyond current offerings.

CONCLUSION

ISRAs are critical for organisations in that they establish an ideal level of security, designed to reduce the impact or probability of a security incident taking place. Through the application of an ISRA method, organisations will identify their critical information assets, their threats and vulnerabilities. These activities, under the 'risk identification' phase of an ISRA method, aim to produce an accurate, holistic inventory of organisational information assets. However, a significant issue is that current risk identification perspectives are focused upon technical infrastructure. This presents a limited view of an organisation's important assets as it discounts the information assets created and applied through practice. Issues such as asset leakage, user-created assets and critical knowledge are all important factors that are not handled by current ISRA methods. Therefore, a business practice perspective has been proposed to form a complete view of an organisation's systems through a process-oriented view. It is suggested that if this perspective is adopted, organisations would hence identify assets at a much deeper level of granularity, producing a much more complete inventory of information assets. By examining worker routines, the leakage of information assets as part of their activities and those assets that are unofficially created to support tasks, a much richer view of an organisation's assets and vulnerabilities will emerge. Likewise with knowledge: while previously not examined rigorously by existing methods, a practice perspective could identify and analyse critical process knowledge that could lead to separate, knowledge management-inspired treatment plans. Though this paper has focused upon the literature within this topic area, we have presented a series of propositions for further study to further explore the effectiveness this practice-oriented perspective can offer organisations.

REFERENCES

Ahmad, A., T. Ruighaver, et al. (2005). 'An Information-Centric Approach to Data Security in Organisations'. Tencon 2005: 2005 IEEE Region 10, Melbourne, Australia.

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

Alberts, C., A. Dorofee, et al. (2004). *Introduction to the OCTAVE Approach*. Pittsburgh, Carnegie Mellon Software Engineering Institute.

AS/NZS (2004). *HB 231 Information security risk management guidelines*, Standards Australia/ Standards New Zealand

Backes, M., B. Pfitzmann, et al. (2003). *Security in Business Process Engineering*. Business Process Management, Springer Berlin/ Heidelberg.

Baskerville, R. L. (1991a). "Risk Analysis as a Source of Professional Knowledge." *Computers & Security* 10(8): 749-764.

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

Bernard, R. (2007). "Information Lifecycle Security Risk Assessment: A tool for closing security gaps." *Computers & Security* 26: 26-30.

Blakely, B., E. McDermott, et al. (2002). 'Information Security is Information Risk Management'. *NSFW '01*, Clourcroft, New Mexico, USA.

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

den Braber, F., I. Hogganvik, et al. (2007). "Model-based security analysis in seven steps - a guided tour to the CORAS method." *BT Technology Journal* 25(1): 101-117.

Brown, J. S. and P. Duguid (2002). *The Social Life of Information*, Harvard Business School Press.

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

Desouza, K. C. and G. K. Vanapalli (2005). 'Securing Knowledge in Organisations'. *New Frontiers of Knowledge Management*, Palgrave Macmillan.

Dhillon, G. (2007). *Principles of Information Systems Security: Text and Cases*. Hoboken, NJ, John Wiley & Sons, Inc.

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

Eloff, J. H. P. and M. M. Eloff (2005). "Information Security Architecture." *Computer Fraud & Security* 2005(11): 10-16.

Farris, G. F. (1979). "The Informal Organisation in Strategic Decision-Making." *International Studies of Man and Organisation* 9(4): 37-62.

Gerber, M. and R. von Solms (2005). "Management of risk in the information age." *Computers & Security* 24(1): 16-30.

Gold, A. H., A. Malhotra, et al. (2001). "Knowledge Management: An Organisational Capabilities Perspective." *Journal of Management Information Systems* 18(1): 185-214.

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

Hamilton, C. R. (1999). "Risk management and security." *Information Systems Security* 8(2): 69-79.

Herrmann, P. and G. Herrmann (2006). "Security requirement analysis of business processes." *Electronic Commerce Research* 6(3-4): 305-335.

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

Jones, A. (2005). "How much information do organisations throw away?" *Computer Fraud & Security* (3): 4-9.

Jones, A. and D. Ashenden (2005). *Risk Management for Computer Security*. Oxford, Elsevier Butterworth-Heinemann.

Kokolakis, S. A., A. J. Demopoulos, et al. (2000). "The use of business process modeling in information systems security analysis and design." *Information Management and Computer Security* 8(3): 107-116.

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

Merkow, M. and J. Breithaupt (2006). *Information Security Principles and Practices*. Upper Saddle River, New Jersey, Pearson Prentice Hall.

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

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

Pfanner, E. (2007). *Data Leak in Britain Affects 25 Million*. The New York Times. New York.

Pipkin, D. L. (2000). *Information Security - Protecting the Global Enterprise*. Upper Saddle River, New Jersey, Prentice Hall PTR.

Ponemon, L. (2006). *Confidential Data at Risk*, Ponemon Institute.

Reid, R. C. and S. A. Floyd (2001). "Extending the Risk Analysis Model to Include Market-Insurance." *Computers & Security* 20(4): 331-339.

Rohrig, S. (2002). 'Using Process Models to Analyse Health Care Security Requirements'. *International Conference on Advances in Infrastructure for e-Business, e-Education, e-Science and e-Medicine on the Internet*, L'Aquila, Italy.

Rohrig, S. and K. Knorr (2004). "Security Analysis of Electronic Business Processes." *Electronic Commerce Research* 4(1-2): 59-81.

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

Maynard, S. and A. B. Ruighaver (2003). 'Development and Evaluation of Information Systems Security Policies'. *Information Systems: The Challenges of Theory and Practice*. M. G. Hunter and K. K. Dhanda. Las Vegas, Information Institute: 366-393.

Sasse, M. A. & I. Flechais (2005). 'Usable Security: Why do we need it? How do we get it?'. *Security and Usability*, O'Reilly Media: 13-30.

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.

Scheepers, R., K. Venkitachalam, et al. (2004). "Knowledge strategy in organisations: refining the model of Hansen, Nohria and Tierney." *Journal of Strategic Information Systems* 13(3): 201-222.

Schultze, U. and D. E. Leidner (2002). "Studying Knowledge Management in Information Systems Research: Discourses and Theoretical Assumptions." *MIS Quarterly* 26(3): 213-242.

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

Shedden, P., T. Ruighaver, et al. (2006). 'Risk Management Standards - the Perception of Ease of Use'. *The 5th Security Conference*, Las Vegas, Nevada, USA.

Shedden, P., R. Scheepers, et al. (2009). "Towards a Knowledge Perspective in Information Security Risk Assessments - an Illustrative Case Study". *20th Australasian Conference on Information Systems, Melbourne*.

Shedden, P., R. Scheepers, et al. (2011). "Incorporating a Knowledge Perspective into Security Risk Assessments", *VINE Journal of Knowledge Management*. Article in press.

Siegel, C. A., T. R. Sagalow, et al. (2002). "Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security." *Information Systems Security* September/ October: 33-49.

Siponen, M. T. (2005). "Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods." *Information and Organisation* 15.

Slay, J. and A. Koronios (2006). *Information Technology Security & Risk Management*. Milton, Wiley.

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: 185-202.

Stacey, T. R. and R. E. Helsley (1996). "Identifying information security threats." *Information Systems Security* 5(3): 50-59.

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

Straub, D. W. and R. J. Welke (1998). "Coping With Systems Risk: Security Planning Models for Management Decision Making." *MIS Quarterly* 22(4): 441-469.

Stolen, K., F. den Braber, et al. (2002). 'Model-based risk assessment - The CORAS approach'. *iTrust Workshop*.

Tan, T., A. B. Ruighaver, et al. (2003). 'Incident Handling: Where the need for planning is often not recognised'. *1st Australian Computer, Network and Information Forensics Conference*, Perth, Western Australia.

West, S., L. S. Crane, et al. (2002). *OCTAVE-DITSCAP Comparative Analysis*. Fort Detrick, Fredick, U.S. Army Medical Research and Material Command.

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

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

Yue, W. T., M. Cakanyildirim, et al. (2006). "Network externalities, layered protection and IT security risk management." *Decision Support Systems* 44.

Zack, M. H. (1999). "Developing a knowledge strategy." *California Management Review* 41(3): 125-145.