Communications of the Association for Information Systems

Volume 39 Article 15

9-2016

Asset Identification in Information Security Risk Assessment: A Business Practice Approach

Piya Shedden
Deloitte Australia, pishedden@deloitte.com.au

Atif Ahmad
University of Melbourne

Wally Smith
University of Melbourne

Heidi Tscherning
Deakin University

Rens Scheepers
Deakin University

Recommended Citation
Shedden, Piya; Ahmad, Atif; Smith, Wally; Tscherning, Heidi; and Scheepers, Rens (2016) "Asset Identification in Information Security Risk Assessment: A Business Practice Approach," *Communications of the Association for Information Systems*: Vol. 39 , Article 15.
DOI: 10.17705/1CAIS.03915
Available at: http://aisel.aisnet.org/cais/vol39/iss1/15

Communications of the Association for Information Systems

Research Paper ISSN: 1529-3181

Asset Identification in Information Security Risk Assessment: A Business Practice Approach

Piya Shedden
Deloitte Australia
pishedden@deloitte.com.au

Atif Ahmad
Department of Computing & Information Systems, University of Melbourne

Wally Smith
Department of Computing & Information Systems University of Melbourne

Heidi Tscherning
Department of Information Systems and Business Analytics
Deakin University

Rens Scheepers
Department of Information Systems and Business Analytics
Deakin University

Abstract:

Organizations apply information security risk assessment (ISRA) methodologies to systematically and comprehensively identify information assets and related security risks. We review the ISRA literature and identify three key deficiencies in current methodologies that stem from their traditional accountancy-based perspective and a limited view of organizational "assets". In response, we propose a novel rich description method (RDM) that adopts a less formal and more holistic view of information and knowledge assets that exist in modern work environments. We report on an in-depth case study to explore the potential for improved asset identification enabled by the RDM compared to traditional ISRAs. The comparison shows how the RDM addresses the three key deficiencies of current ISRAs by providing: 1) a finer level of granularity for identifying assets, 2) a broader coverage of assets that reflects the informal aspects of business practices, and 3) the identification of critical knowledge assets.

Keywords: Information Security, Risk Assessment, ISRA Methodologies, Rich Description Method.

This manuscript underwent editorial review. It was received 01/21/2016 and was with the authors for 1 month for 2 revisions. Jackie Rees Ulmer served as Associate Editor.

1 Introduction

To sustain competitive advantage in a knowledge economy, organizations need to protect their knowledge and information assets such as intellectual property (IP), trade secrets, product blueprints and business strategies (Ahmad, Bosua, & Scheepers, 2014a). A comprehensive and effective information security management (ISM) strategy begins with an accurate information security risk assessment (ISRA). An effective ISRA attempts to provide a prioritized estimation of the likelihood and impact of a range of security scenarios, with each scenario considering potential threats to organizational assets and existing protective controls (Shedden, Ruighaver, & Ahmad, 2010a; Ahmad, Maynard, & Park 2014b). ISRAs then guide the strategic selection of security controls to protect information resources (Dhillon & Backhouse, 2001). Established ISRA methodologies such as the operationally critical threat, asset, and vulnerability evaluation (OCTAVE), facilitated risk analysis process (FRAP), platform for risk analysis of security-critical systems (CORAS), and central-communication-and-telecommunication-agency risk analysis and management method (CRAMM) have been developed with supporting tools and documentation that tailor control implementations to each organization (Alberts & Dorofee, 2002; den Braber, Hogganvik, Lund, Stølen, & Vraalsen, 2007; Peltier, 2001; Stølen et al., 2002; Yazar, 2002).

However, recent studies into the practice of applying ISRA methodologies in organizations report that they take a limited perspective of organizational "assets", which ultimately leads to inaccurate security risk assessments. We can identify three significant deficiencies. First, ISRAs typically adopt a traditional accountancy-based view of assets that sees them as discrete and relatively static categories of information that one can enumerate for auditing purposes, which leaves ISRAs with a coarse-grained view of relevant assets and the related risks. Second, ISRAs tend to be restricted to those assets that are visible in a formal business process view and do not take a sufficiently social and organizational perspective that recognizes the informal work practices and workarounds in which assets exist and evolve. Third, the strong focus on information that ISRAs adopt can lead analysts to neglect the less visible but essential organizational knowledge that creates and supports it. Taking insights from the knowledge management (KM) field, we need to identify knowledge as a kind of asset worthy of protection, notwithstanding its less tangible existence in the "fluid mix of framed experiences, values, contextual information and expert insight" (Davenport & Prusak, 1998, p. 5).

Given these three areas of deficiency, we address the following question in this paper:

RQ: How might the identification of information and knowledge assets be improved in ISRAs?

Broadly, we argue that ISRA methodologies must incorporate a richer perspective of business practice to be able to identify and protect important information and knowledge. To this end, we propose a novel rich description method (RDM) that adopts a richer and more holistic view of assets and use appropriate data collection and analysis techniques to uncover them.

The paper proceeds as follows. In Section 2, we overview the ISM literature and clarify the three broad limitations of asset identification in current ISRAs. In Sections 3 and 4, we report a case study of an engineering company (ArchiFirm) to compare the application of an existing risk assessment methodology (Section 3) with the application of our rich description method (RDM). We use the RDM to construct qualitative descriptions of business processes that capture the rich context behind the interactions, relationships, motivations, and desires of various actors in the work of ArchiFirm. In Section 5, we compare the findings of the traditional ISRA and our novel RDM and argue that the RDM provides a valuable complement to existing approaches that addresses the three deficiencies identified. In Section 6, we discuss the paper's contributions to theory and implications for further research and practice. Finally, in Section 7, we conclude the paper.

2 ISRMs and Asset Identification

Information security risk management methodologies (ISRMs) are the means by which organizations systematically identify and actively protect their information assets and, thereby, attempt to minimize tangible and intangible losses (Blakley, McDermott, & Geer, 2001; Eloff & Eloff, 2005; Reid & Floyd, 2001). Through the phases of a traditional ISRM, an organization develops a plan to achieve a desired and cost-effective future state of information security (Standards Australia, 2004a). This plan specifies choices about what controls to implement so as to mitigate or reduce security risks (Shedden et al., 2010a).

When following an ISRM, the organization needs to identify the following: the assets critical for its operations; the threats to each asset's confidentiality, integrity, and availability; and asset vulnerabilities (Alberts & Dorofee, 2002; den Braber, Hogganvik, Lund, Stølen, & Vraalsen, 2007; Finne, 2000; Stølen et al., 2002). The organization then quantifies each risk in terms of its consequences and likelihood of occurring (Peltier, 2001), which produces a prioritized list of risks for further action (Alberts & Dorofee, 2002; Roper, 1999). Managers must then consider how to control the higher priority risks by selecting one of four basic strategies: avoidance, mitigation, transference or acceptance (Whitman & Mattord, 2014). Finally, the organization must continue to monitor its situation after implementing controls to ensure that they are maintained and actually achieve the desired level of coverage (Standards Australia, 2004a).

2.1 The Information Security Risk Assessment (ISRA)

In this study, we are concerned with just the information security risk assessment (ISRA) part of a full ISRM. Though many studies have used the term "risk assessment" interchangeably with other terms, including "risk analysis" and "risk evaluation" (Frosdick, 1997), we define an ISRA as comprising context-establishment, risk-identification and risk-analysis, but we exclude risk control (Dhillon, 2007; Stoneburner, Goguen, & Feringa, 2002).

ISRAs, then, focus on how an organization identifies individual *risks* defined as the *probability of a negative occurrence* that threatens the achievement of objectives (Standards Australia, 2004b; Slay & Koronios, 2006). Risks are assessed and expressed in terms of how likely they will occur and the impact if they did (ISO/IEC, 2001; Stoneburner et al., 2002). The information security literature notes that risks exist at the intersection of three things: assets, threats, and vulnerabilities (Cooper & Johnson, 2003; Gerber & von Solms, 2001; Jones & Ashendon, 2005; Kokolakis, Demupoulos, & Kiountouzis, 2000; Roper, 1999). Identifying risks typically comprises two sub-phases: 1) identifying assets and 2) identifying threats and vulnerabilities. In other words, identifying risks entails providing a list of critical information assets the organization needs to protect and identifying their vulnerabilities and potential threats that could exploit the assets (Reid & Floyd, 2001).

2.2 Understanding the Significance of Asset Identification

What counts as an information asset is a critical decision in an ISRA. Information assets are typically understood to be any information of value to an organization (Peltier, 2001) that, therefore, requires some measure of protection (Standards Australia, 2004a). The ISM literature typically sees information assets as: hardware, software, data, and information; people who support and use the IT system; communications equipment; and various services, such as utilities (Alberts, Dorofee, Stevens, & Woody, 2003; Standards Australia, 2004b; Hamilton, 1998; Stoneburner et al., 2002; Warren & Hutchinson, 2003). Because they are a primary source of value, researchers regard information assets as a sensible unit of analysis when conducting ISRMs (Alberts et al., 2003; den Braber et al., 2007; Moody & Walsh, 1999; Peltier, 2001; Roper, 1999).

The first step in the ISRA process is to systematically discover and select all relevant information assets that the organization holds. One uses the same system of categorization as described for ISM above (Alberts et al., 2003; Bass & Robichaux, 2001; Landoll & Landoll, 2005; Lichtenstein, 1996; Visintine, 2003). Organizations must identify all information assets in the scoped system to inform accurate decisions in the future (Standards Australia, 2004a). Each information asset in an organization will have some level of value (Spinellis, Kokolakis, & Gritzalis, 1999). However, budgetary and time constraints mean that assessment of risks cannot be made for all of them (Roper, 1999). The ISRA process must decide which information assets are essential or critical for the system under review (Alberts et al., 2003; Cooper & Johnson, 2003).

Once an organization has identified its critical information assets, it attempts to accurately and completely define the threats to each (Stacey, Halsley, & Baston, 1996). Here, one needs to identify the outcomes of a successful attack on each asset, such as the possibilities for destruction, modification/corruption, or interruptions to access or operation (Farahmand, Navathe, Enslow & Sharp, 2003). One determines the specific impacts with reference to the three important states of the affected information: its confidentiality, integrity, and availability.

ISRAs are process driven and guide organizations through the steps of understanding and assessing their information security risks. Popular ISRA methodologies include FRAP, CRAMM, COBRA, OCTAVE, and CORAS (Alberts & Dorofee, 2002; den Braber et al., 2007; Dhillon, 2007; Peltier, 2001; Yazar, 2002).

Although these methodologies differ in their composition, order, and depth of activities, they generally follow a three-stage pattern: 1) establish the context, 2) identify the risks, and 3) analyze the risks (Dhillon, 2007; Shedden et al., 2010; Whitman & Mattord, 2014). The outcome of the risk assessment depends on the organization's setting the correct scope for assessing risks (the first phase), generating an accurate inventory of assets and the associated risks to those assets (second phase), and accurately estimating the probabilities and impacts for each risk (third phase).

2.3 Limitations of Asset Identification

The ISM literature generally agrees that ISRA outcomes are frequently inaccurate because of shortcomings in the early asset identification phase (Siponen, 2005b; Spears, 2006; Webb, Ahmad, Maynard, & Shanks, 2014; Zafar & Clark, 2009). In particular, Salmela (2008, p. 2) and Dhillon and Backhouse (2001, p. 142) note that ISRA methodologies tend to focus on technological assets such as hardware and software rather than people, knowledge, and practice.

We contend that the asset identification phase of current ISRAs has three general deficiencies. First, the phase results in a coarse level of granularity of assets. When applying traditional ISRA methodologies, many organizations tend to default to a high-level assets (Shedden et al., 2010). For example, they often identify a whole information system, such as a database or content management system, as a single asset. In this way, they treat these complex technologies as "black boxes" without distinguishing their various functions, modes of use, and different areas of informational content. Consequently, they cannot easily identify particular risks associated with particular component elements. This inability to correctly identify risks results partly from inappropriately applying the methodologies and partly from the methods themselves not providing guidance to drill down to a deeper level of detail (Lichtenstein, 1996; Shedden et al., 2010). An organization taking this approach might be successful in identifying the higher-level, generic and broader risks around their broadly-defined information systems. However, it would not readily discover those risks specific to particular information assets, such as individual servers, hot-desk laptops, printer rooms, social media functions, and so on. In reality, each of these neglected elements might be subject to their own special threats and vulnerabilities and, hence, have a unique risk profile.

Second, traditional asset identification identifies formally recognized assets but neglects the co-existing informal activities that are typically necessary for the organization to work in practice. Current ISRA methodologies consider assets as discrete objects and largely ignore the social and processual aspects of information systems (Ahmad et al., 2005; Rohrig & Knorr, 2004; Spears, 2006). Historically, information security focused on physical, mechanical issues related to procedurally and physically separate batch-processing facilities (Gerber & von Solms, 2005). But information systems today are deeply embedded in a rich social environment and influenced by user behaviors that are part of informal work practices (Brown & Duguid, 2002; Dhillon & Backhouse, 2001; Spears, 2006). As such, we need a more holistic socio-organizational view of security (Dhillon & Backhouse, 2001; Shedden, Scheepers, Smith, & Ahmad, 2011; Siponen, 2005a) because these social, practice-based aspects bring with them distinctive and significant risks. In particular, information assets are not static—they evolve and change as people use and create them dynamically as part of their formal and informal work routines and even in formal business processes (Ahmad, Ruighaver, & Teo, 2005; Brown & Duguid, 2002; Farris, 1979). In reality, work environments are flexible and even chaotic, and individuals pursue workaround activities and shortcuts using their own initiative (Sasse & Flachais, 2005). If ISRAs do not consider actual practices, they clearly have limited value for improving an organization's risk profile and, consequently, will most often only identify high level and abstract information assets.

Third, traditional asset identification does not recognize knowledge assets as distinct and important entities. By knowledge asset, we mean a distinct category of what the organization knows collectively that enables it to perform competitively. In an in-depth case study of a software engineering firm, Shedden et al. (2011) explored the limitations of the traditional asset perspective. They applied a traditional ISRA to the organization and examined the resulting outcome from a knowledge perspective. They found that the risks identified by the traditional ISRA belonged to four categories: 1) systems, 2) data, 3) people, and 4) applications. Further, they found that the traditional view of information assets did not allow analysts to capture the critical tacit and explicit knowledge held both individually and in a distributed form. While the traditional asset-oriented view simply pointed out security risks related to key individuals, it failed to identify the specific vulnerabilities resulting from the poor distribution of sensitive knowledge and a related over-dependency on key knowledge-holders.

3 Case Study of ArchiFirm Part 1: Applying a Traditional ISRA

The three deficiencies in current ISRAs point to the need to modify and extend the practice of information security risk assessment. We now report a study to explore how one might do so. We designed the study as a case study of information security asset identification in a selected real organization to compare two approaches: 1) a traditional ISRA of the sort described above and 2) a new approach that we call the rich description method (RDM) and that uses more probing data-collection and analysis techniques drawn from qualitative field research methods. We intended to discover if these more probing techniques could effectively address the three limitations of current ISRAs. We adopted the case study method given its suitability to capture complex real world phenomena, such as organizational risk (Darke, Shanks, & Broadbent, 1998; Dubé & Paré, 2003; Yin, 2009).

This section reports part 1 of the case study in which we applied a traditional ISRA. In Section 3.1, we provide the background to the case study organization, and, in Section 3.2, we describes the selected traditional ISRA that we applied and briefly illustrates the kind of assets that that methodology identified. In Section 4, we report part 2 of our study to develop and apply our RDM that sought to go beyond the scope of the traditional ISRA.

3.1 The Case Study Organization: ArchiFirm

Our case study examined an Australian civil engineering company ("Archifirm") that provides soil testing, drafting, and engineering services to the state of Victoria's high-volume house-building sector. We chose ArchiFirm for three main reasons. First, it is a small company of about 60 staff, which allowed us to gain an understanding of its overall operation and context in a reasonable timeframe. Second, ArchiFirm's work involved communicating across multiple sites with many kinds of expertise; hence, its reliance on information flow and knowledge management were highly visible and accessible to study. Third, ArchiFirm's staff recognized information security issues. This awareness was heightened because ArchiFirm had recently lost a key employee with critical knowledge necessary to operate a core business process. As a result of this incident, ArchiFirm recognized that its existing security processes were inadequate and, therefore, had already begun to investigate ISRA methodologies. As such, ArchiFirm provides a representative case (see Yin, 2009; Seddon & Scheepers, 2012) but also one that was readily accessible and receptive to our plan to assess and compare ISRA methodologies.

ArchiFirm had two key departments: a soils department with 10 employees, and an engineering department with 40 employees. We focus on a key business process, described as the soils and engineering process, which spans across these two departments. The soils department conducted on-site soil tests to determine land composition, which influenced subsequent engineering decisions. The engineering department then developed drafts of a structure's foundations and beams. Depending on the soil type, engineers then calculated the dimensions of these structural components to best support the future building. An office manager headed the administrative function of the organization that ensured that work flowed smoothly through the office and identified bottlenecks. Both soil and engineering personnel needed to be familiar with client-specific requirements. These requirements dictated client preferences on the types of materials in the supporting structure, such as metal and wood, and how they should format reports.

The soils and engineering (SE) process represented an opportunity to study the three areas of limitation in standard ISRAs that we identify in Section 2. The SE process depended on various and significant forms of expert knowledge. Early observations indicated significant flexibility and workarounds were necessarily to ensure that the formal business process worked smoothly in practice. Further, the SE process represented the organization's primary purpose and was the means by which the firm generated its revenue. Indeed, if this process did not deliver accurate calculations and reliable data for decision making, the firm risked structural instability, delays in construction, additional unnecessary expenses, and significant reputational loss in a highly competitive field. Also significant was that, due to the nature of work, the integrity of the process was important for the health and safety of employees.

From a competitiveness perspective, ArchiFirm has accrued considerable organizational knowledge in the context of this key business process. In particular, over time, the organization has compiled a unique "recipe book" comprising a range of different soil templates. These templates, associated learning, and various informal works practices are central to ArchiFirm's ongoing competitiveness.

3.2 Applying a Traditional ISRA Methodology: OCTAVE-S

As a representative exemplar of traditional ISRA methodologies, we applied the operationally critical threat, asset, and vulnerability evaluation methodology for small organizations (OCTAVE-S) to our case organization. OCTAVE-S is a subset of a larger ISRA methodology, OCTAVE, developed by Carnegie Mellon University as a comprehensive, asset-focused approach to identifying and treating organizational information security risks (Alberts et al., 2003, p. 3). OCTAVE is a self-directed ISRA methodology that allows organizations to self-study and conduct risk assessments so that they can capture their own technical knowledge (Alberts et al., 2003). The methodology claims to leverage people's knowledge of their organization's practices and processes to determine its current state of security readiness. Risks to the identified critical assets determine which areas of improvement are needed and inform the development of a security strategy (Alberts et al., 2003, p. 3). While some ISRA methodologies focus on technology, OCTAVE-S focuses on organizational risk and practice-related issues. Hence, one might expect OCTAVE-S to do relatively well on the areas of limitation that we set out to investigate.

Other ISRA methodologies include CRAMM (ver. 4), CORAS, FRAP, OCTAVE, COBRA, and international standards, such as AS/NZS 4360:2004 (Alberts & Dorofee, 2002; Standards Australia, 2004b; Peltier, 2001; Stoneburner et al., 2002; Yazar, 2002). We conducted a feasibility study of these methods to determine which would be the most appropriate for our study. Ultimately, we selected the OCTAVE-S methodology due to its rigor and alignment with industry and research ISRA methodology "best practice" (Shedden et al., 2010). OCTAVE-S is also widely applied with good support for its validity (Satchidananda & Shanthamurthy, 2004; West, Crane, & Andres, 2002; West & Andrews, 2003).

Table 1. Risk Analysis Team Participants in OCTAVE-S Workshops

Participants	Number of sessions	Total duration
IT developer Engineering-IT partner Office manager	13	14 hours

Because OCTAVE-S is self-directed, the organization selects three to five individuals to form a risk-analysis team. The team then identifies and analyzes its critical risks to establish organization-wide security strategies and asset-based risk-mitigation plans (Alberts et al., 2003). The method helps the team to identify critical information assets based on their alignment with business objectives. Subsequently, OCTAVE-S conforms to the typical ISRA phases, including context establishment, risk identification, risk analysis, and risk control. It is structured around three phases that contain one or more "processes" with multiple "activities". In phase 1, one constructs asset-based threat profiles. In phase 2, one identifies vulnerabilities by examining computing infrastructure in relation to critical assets. Finally, in phase 3, one develops a security strategy by identifying and analyzing risks and then develops protection and mitigation plans.

We facilitated the implementation of OCTAVE-S at ArchiFirm by guiding the company to establish a riskanalysis team as Table 1 shows. We facilitated 13 workshop sessions with this team to work through the prescribed list of formal, structured questions, with associated predefined templates and worksheets to identify and analyze the firm's security risks. As OCTAVE-S requires, the team provided a balance between an operational and organizational perspective, an information-flow perspective, and an IT perspective (Alberts et al., 2003). The engineering-IT partner and IT developer made up the IT department of the firm. The engineering-IT partner fulfilled a top-management function, including security management and network administration. The IT developer performed more technical tasks, including developing and managing the organization's database and website, providing support for staff desktops, and handling incidents. The office manager brought substantial knowledge of the business by describing ArchiFirm's operations and information assets across all departments. The IT developer also possessed strong knowledge of departmental information asset requirements throughout the business. Table 2 provides an illustrated sample of the critical assets identified through the implementation of OCTAVE-S at ArchiFirm.

Table 1. Illustrative Sample of Critical Assets Identified through OCTAVE-S

Critical asset	Asset type	Rationale for selection
Database system	System	The database contained all past and current job information. Without the database, ArchiFirm would be unable to register, track, and update orders.
Engineering software	Services/ application	Engineering software refers to AutoCAD and CadeComp, two critical applications required by the drafters and engineers in the day-to-day production of the drafts. ArchiFirm would be incapable of completing jobs without these applications.
Desktop computers	System	The desktops were the means by which all people in the organization performed their work. If a large number of desktops were rendered inoperable, employees would be unable to access critical software functions and work could not progress.
Web system	System	The Web system was the means by which most of ArchiFirm's clients booked jobs and observed their progress. If the web system failed, ArchiFirm would not be able to receive the majority of its job orders.
Backups	Information	Backups were integral to ArchiFirm's ongoing operations. The backups were copies of all information flowing through ArchiFirm's systems. If any information was lost, as happened frequently, the firm used the backups to restore past information states to ensure continued operations.

4 Case Study of ArchiFirm Part 2: Applying a Rich Description Method

Part 2 of our case study concerned developing and applying a RDM. For simplicity, we describe what the RDM involved in advance of illustrating its findings, although, in practice, we refined it via conducting the investigation and it is itself an output of the study. One has many ways of using rich methods of data collection to enhance ISRAs, and, thus, we present our particular RDM as illustrating a wider class of approaches. We focused on determining if this kind of data collection and analysis might overcome the identified shortcomings of ISRAs. Figure 1 overviews the six activities of our RDM, including data collection, analysis through rich descriptions, and outputs. Before explaining these steps in detail, we describe the rationale and motivation for our RDM in Section 4.1. In Sections 4.2 to 4.5, we outline each of the activities of Figure 1 and provide illustrations of the resulting data and analysis.

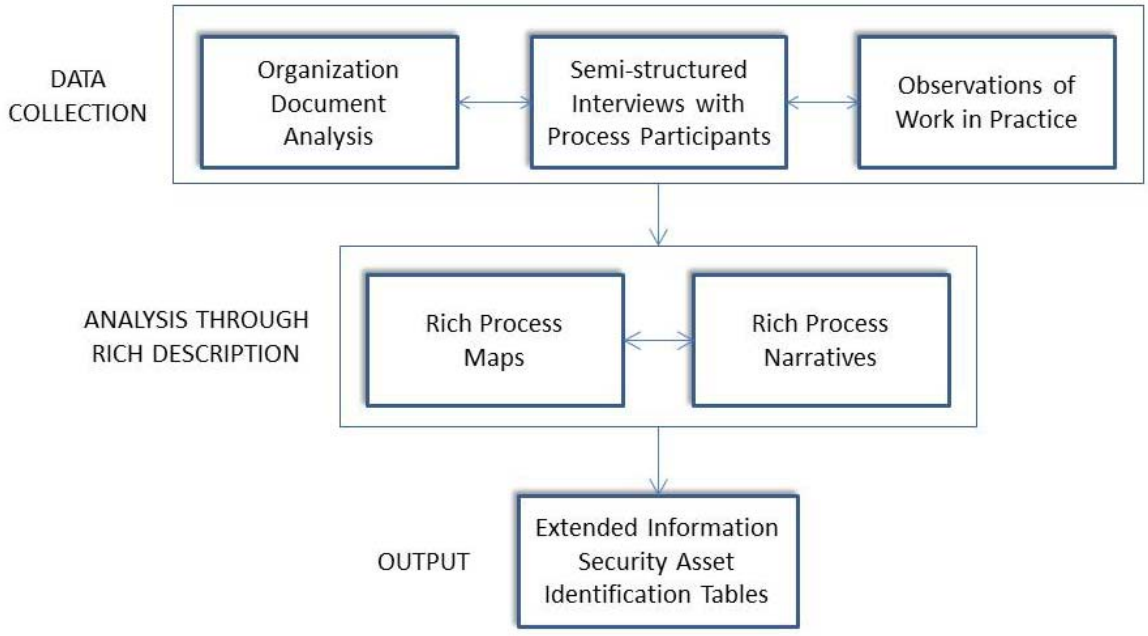


Figure 1. Rich Description Method: Data Collection, Analysis, and Output

4.1 Rationale for a Rich Description Method

Our proposed RDM relies on recognizing the distinction between the formal and informal aspects of organizations and the distinction's implications for information security. By formal aspects, we mean the official view of the organization captured in such things as structure charts, designated roles, duty statements, and key business processes (Farris, 1979). By informal aspects, we mean the unofficial working patterns, attitudes, and dispositions of staff that arise and exist through the organization's social fabric. The concept of "business practice" is central to understanding the informal aspect of organizations (Hislop, 2009). While business process refers to a set of formally known activities and tasks that staff carry out (Davenport & Prusak, 1998), business practice refers to interrelated but distinct social patterns and informal ways of working (Sasse & Flechais, 2005) that staff create through improvisation and propagate through storytelling and shared experiences (Brown & Duguid, 2002). While a process perspective concerns the way organizations conduct work in a routine and predictable manner (Brown & Duguid, 2002), a practice perspective draws our attention to the various workarounds, informal flows of information, and unofficial activities that are needed to get work done. From a security point of view, such informal actions have implications for the security environmen, and might result, for example, in the accidental leakage of information or the duplication and distribution of information assets in a way not picked up by traditional ISRA methods that focus purely on the formal side of the organization.

While traditional ISRAs focus on the formal and easily reportable elements of organizations, the RDM we propose here draws attention to both formal and informal aspects and the relationship between them. On the formal side, our RDM focuses on business processes as a framework for its investigation. But, around this, it explores related informal aspects of work via in-depth interviews and detailed analyses in the form of rich process narratives and rich process maps (see Figure 1). The term "rich description" has its grounding in soft systems methodology's (SSM) "rich pictures" and ethnographic "thick" descriptions (Geertz, 1994). Like these techniques, our rich descriptions attempted to capture the informal and subtle dimensions of actors' organizational life, including their actions, beliefs, intentions, relationships, motivations, and desires (Denzin, 2001). The act of developing a rich description, then, offers to immerse the information security analyst into the organizational environment beyond the scope of a typical ISRA project while staying in its practical time and budgetary constraints.

In devising an RDM, we focused on identifying critical organizational knowledge as a kind of valuable asset that organizations need to protect. However, this knowledge typically resides in informal business practices (Brown & Duguid, 2001; Hislop, 2009). Although explicit knowledge is likely to be formally documented and available to traditional ISRAs, vital tacit knowledge will remain hidden. By definition, one cannot articulate tacit knowledge to ISRA analysts, and it is typically evident only in situations where one applies and acquires it (Hislop, 2009; Nonaka, 1994; Tsoukas, 1996). That is, tacit knowledge is heavily grounded in organizational practice, and, typically, one cannot separate this kind of "knowing" from "doing" (Cook & Brown, 1999; Gherardi, 2000). Likewise, organizations also embed significant and valuable methods for cultivating organizational knowledge in practices. Staff can learn through formal inductions and training, but more often they learn through less visible acts of experimentation and sharing ideas (Hislop, 2009; Nadler & Tushman, 1980). Therefore, much critical knowledge and the mechanisms of acquiring it are likely to be invisible to a traditional ISRA, which confirms the need for an RDM to identify them and their attendant security risks.

4.2 Data Collection for the Rich Description Method: Observation, Interviews, Document Analysis

Our proposed RDM involved six interrelated activities (see Figure 1). In the first stage, we collected data in three concurrent and interrelated steps: we analyzed company documents, observed work in practice, and conducted semi-structured interviews with participants whose work related to the particular business processes under review. The main researcher (the first author) conducted all of these data-collection steps. He conducted the semi-structured interviews with 11 participants, each interviewed several times (see Table 3). Interviews varied in length due to the differing complexity of tasks, activities, and organizational seniority. We formulated questions to be exploratory and to elicit details about the information, knowledge, and operational aspects surrounding each step of the process. Based on information we derived from company documents and from observing work in action, we designed questions to probe information flows, the information lifecycle, work behaviors, and the role of critical knowledge. We found it important to incorporate opportunities for follow-up questions and deeper examination of intriguing responses. Interviews designed and conducted in this way are an effective

means of capturing the rich detail surrounding work practices, particularly of knowledge and the artifacts that individuals use in computer-assisted work (Wood, 1997). The workplace observations augmented the interview data by showing how users engaged in work, especially where tacit knowledge was critical (Wood, 1997). We gathered the main documents relating to ArchiFirm's business processes, including process charts, reports, forms, emails, photographic images, and maps. We found these artifacts to be highly informative about the formal and informal aspects of work and the forms of information that could potentially leak to rivals.

Table 3. Participants in RDM Interviews

Participant role	Department	# of sessions	Interview duration
Accountant	Administration	3	2 hours
Engineering partner	Engineering department	3	2.1 hours
Senior soils report writer	Soils department	4	2.2 hours
Head drafter	Engineering department	2	1.2 hours
IT developer	IT department	4	2.2 hours
IT partner	IT department	3	3 hours
Managing director	Corporate	2	1.6 hours
Office manager	Administration	2	2 hours
Order entry admin	Administration	2	1 hour
Soils partner	Soils department	4	1.8 hours
Soils report writer	Soils department	2	1 hour

4.3 Rich Process Maps

Based on the three forms of data collected (see Figure 1), we constructed a rich description of selected processes at ArchiFirm through two analysis techniques carried out in tandem. First, we constructed rich process maps that we initially drew as standard workflow models using business process modeling notation (BPMN) methodology (e.g., Dumas, La Rosa, Mendling, & Reijers, 2013). BPMN provided a formal view of each process to which we annotated comments about each step's relationship with the informal knowledge and activities of business practices, which Figures 2 and 3 illustrate.

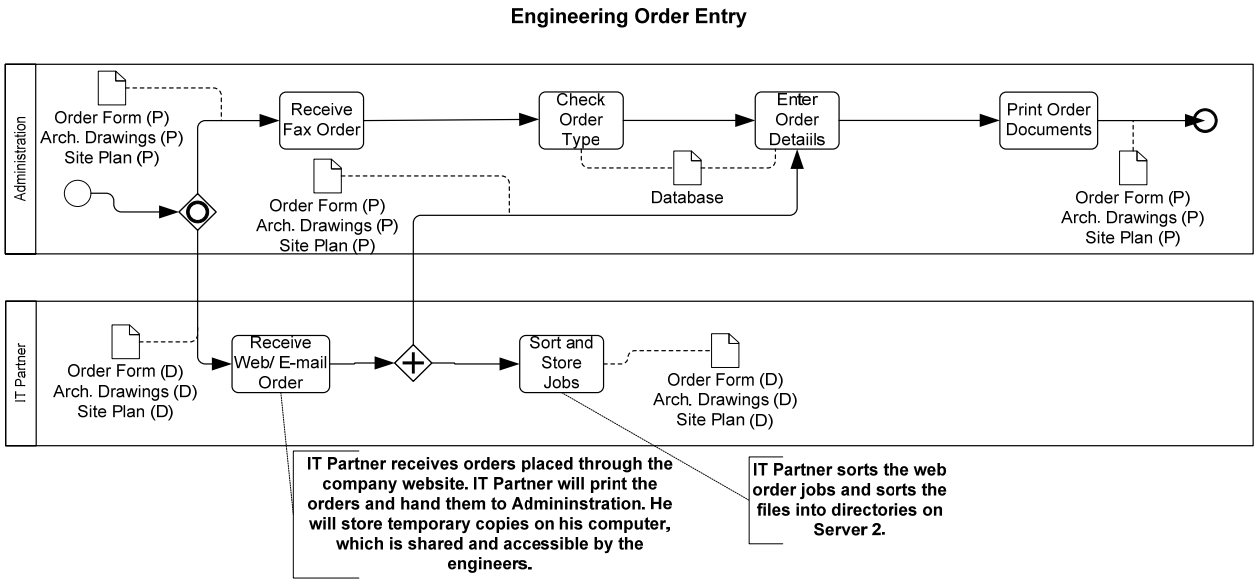


Figure 2. Information Flows in BPMN with Rich Description Markups) (P Denotes a Physical Document and D Denotes a Digital Document)

Using BPMN provided a way to establish a coherent picture of the process and allowed us to explore potential gaps in the evidence. Its diagrammatic representation provided an effective and concise medium to express relationships between processes and practices (Checkland, 2000; McFadzean, 1998; Venters, Cushman, & Cornford, 2002). We used BPMN's "information artifacts" to document the key "containers" of information (Ahmad et al., 2005; Bernard, 2007) around which security threats arose. We labeled the containers with P for "physical" or D for “digital" to make their format explicit as a resource to reason about security risks. Most valuable, however, was our use of annotations in the diagrams to document the informal context around information flows, activities, and information “containers”, which allowed us to make explicit the knowledge requirements for each task and to identify who held that knowledge. We further used annotations to capture details such as the movement of physical information throughout the office buildings and site locations.

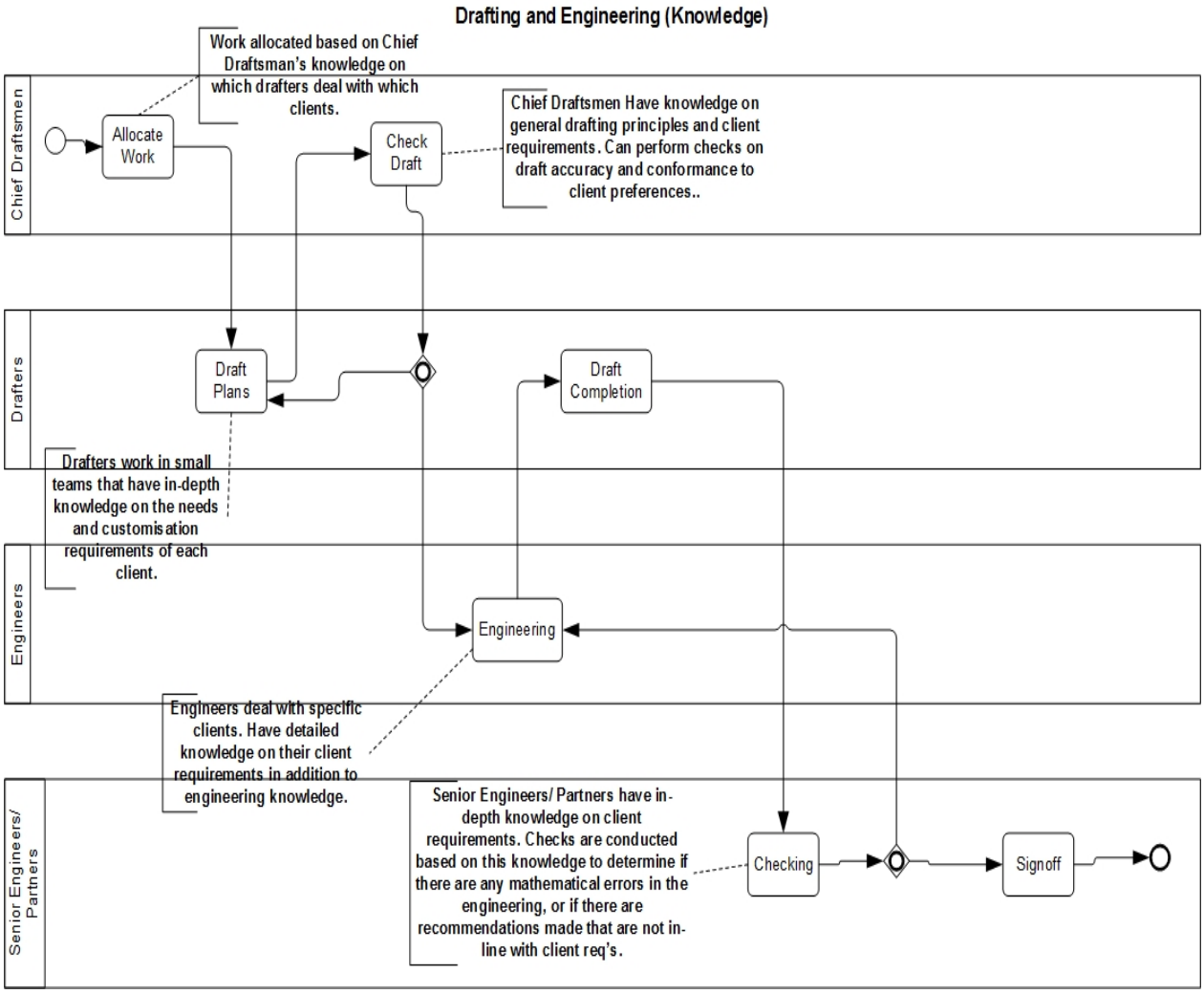


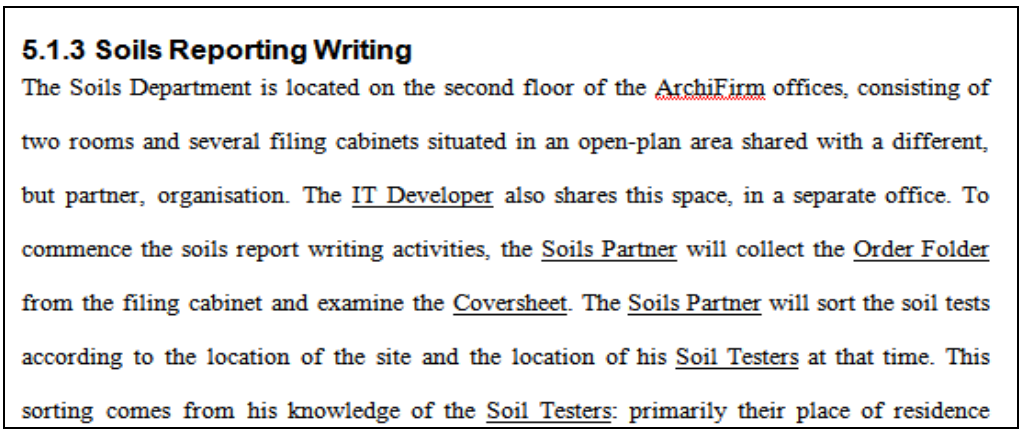
Figure 3. Representing Critical Knowledge in BPMN

We found that attempts to incorporate all information flows, activities, and departments/individuals onto one process map quickly complicated matters. As such, instead, we constructed two kinds of process maps: the first outlined information flows and information containers (e.g., Figure 2) and the second focused on the knowledge requirements for activities (e.g., Figure 3). In this format, we found the diagrams to be useful resources to examine the processes’ security vulnerabilities. For example, we could see the following things more clearly: the transfer of information in either physical and digital form as an official part of the process, the flow of information between containers, where residual copies of the information ended up as the process proceeds, what critical information might be leaked through unofficial work practices, and the criticality and vulnerability of organizational knowledge.

4.4 Rich Process Narratives

In tandem with constructing the rich process maps, we also wrote rich process narratives that comprised story-based accounts of the flow of work (Figure 4 shows an example). These narratives reflected the formal sequence of tasks as captured in the rich process maps, but they were more versatile in being able to capture the idiosyncratic aspects of the informational infrastructure required to perform tasks and the information and data produced, manipulated, disposed of, disclosed, and/or recorded and stored. We wrote narratives to express the experiences of the people performing tasks with respect to the knowledge deployed, information used, and other contextual elements. In this way, we could capture and express the informal aspects of work to a greater extent than with the rich process maps alone.

The identification of the physical settings in which tasks were carried out turned out to be highly relevant to risk assessment. Traditional ISRAs typically neglect this aspect, but we found it to be significant when considering the type and severity of information security risks. While the interview data typically reflected individual perspectives and varied significantly across different levels and areas of the organization, the rich process narratives brought together this evidence into a coherent account. This analysis technique also captured insights into the informal aspects of surrounding work practices.



5.1.3 Soils Reporting Writing

The Soils Department is located on the second floor of the ArchiFirm offices, consisting of two rooms and several filing cabinets situated in an open-plan area shared with a different, but partner, organisation. The IT Developer also shares this space, in a separate office. To commence the soils report writing activities, the Soils Partner will collect the Order Folder from the filing cabinet and examine the Coversheet. The Soils Partner will sort the soil tests according to the location of the site and the location of his Soil Testers at that time. This sorting comes from his knowledge of the Soil Testers: primarily their place of residence

Figure 4. Illustrative Passage from a Rich Process Narrative

4.5 Extended Asset Identification Tables

Using both the rich process maps and rich process narratives enabled a more extensive identification of information security assets that the organization needed to protect. Our RDM helped to break down the highly visible physical assets that the risk analysis team identified through OCTAVE-S into their separate components, including specific documents, desktops, servers, and databases. More significantly, the RDM techniques encompassed all these physical “containers” to identify important classes of information and knowledge as critical assets. Through using the rich process maps and rich process narratives, we produced extended asset identification tables that summarized these critical assets as entries in a database.

Shedden et al. (2010) theorize that capturing and analyzing activities in a business process provides a richer view of the information assets required to operate in that activity. Capturing and analyzing these activities involves identifying infrastructural, information, and/or data assets that support, are used by, or are produced by such activities. Furthermore, by analyzing the formal and informal information flows between activities, one can identify potential information leakage from containers and storage devices (as per Ahmad et al., 2005; Bernard, 2007). Table 4 shows examples of entries in an information assets table.

Importantly, by adopting a practice perspective, one can identify critical knowledge. Knowledge is integral to business processes and is typically embedded in an organization’s practices. Therefore, one needs methods to identify critical knowledge assets with sufficient granularity and to pinpoint the risk of that knowledge’s leaking. Table 5 shows examples of entries in a knowledge asset table.

The information asset table (Table 4) lists each identified asset, its type, its official location, and its container. This format is consistent with ISRA methodologies, including OCTAVE-S, but provides an extended list of information assets at a finer level of granularity. The table also shows informal information

assets and their "unofficial" containers and locations. These informal assets form an "information residue", by which we mean the array of unofficial copies that are produced and left behind as a by-product of the formal process. Examples of these unofficial locations include employees' home PCs or removable storage devices. Clearly, these unofficial copies represent sources of potential leakage risk.

We used the knowledge asset table (Table 5) to identify and name the categories of knowledge that were critical to effective operation of the processes under review. Each item of knowledge in the table related to these key business process, which, in turn, underpinned the value of this knowledge to the business. For each knowledge asset, the table describes its explicit and tacit elements and identifies the employees who possessed the knowledge. The table represents a useful resource for the analyst team and for the managers of the critical knowledge that warrants protection. The table also highlights potential vulnerabilities associated with critical knowledge (e.g., knowledge possessed by only one key individual).

Table 4. Representative Entries from an Extended Asset Identification Table (Information Assets)

Asset	Type	Official location	Official container type	# of Copies	Unofficial location(s)	Unofficial container type
Soils faxed order forms	Information	Server 1	Digital	4+	Soil partner's PC, Server 1 (email), Laptops	Digital
Photographs	Information	Folder	Physical	4+	Temporary hard-copies given to co-workers	Physical
Soil report	Information	Server 1	Digital	2+	Soil partner's PC	Digital
AutoCAD	Application	Desktops	Digital	Unknown #	Home computers	Digital
Eng. Excel templates	Application	Desktops	Digital	Unknown #	Home computers	Digital
QuickBooks	Application	Desktop, Laptop	Digital	8	Nil	Nil
Server 1	System	Eng-IT partner's office	Physical	4 (backups)	Engineering-IT partner's desk, car, home	Digital
Backups	Information	On-site storage device on server	Digital	4	Engineering-IT Partner's desk, car, home	Digital

Table 5. Representative Entries from an Extended Asset Identification Table (Knowledge Assets)

Knowledge asset	Possessor of knowledge	Description
Soil test job allocation knowledge	Soils partner	The soils partner knew where his soil testers lived and where they generally performed their work, which made work allocation more efficient by reducing travel times for testers.
Soil report checking knowledge	Soils partner & senior soils report writer	The soils partner and senior soils report writer possessed considerable knowledge of local geology, particularly the soil composition of suburbs that ArchiFirm services. These knowledgeable individuals identified many potential errors.
Client requirements drafting knowledge	Head drafters & drafters	Drafters worked with specific subsets of clients. The cumulative knowledge of each client's situation and requirements were paramount for ensuring high-quality work with few errors.
Process management knowledge	Office manager	The office manager had in-depth knowledge of the process workflows, points of contact, individuals' personal work habits, and bottlenecks. She could diagnose workflow issues early, follow-up lost orders, and re-organize job orders to ensure that ArchiFirm remained productive.
Database maintenance knowledge	IT developer	The IT developer was the only person in ArchiFirm who understood how to operate the database, including its range of functionality, methods of debugging, and general maintenance.

5 Comparative Findings

We now compare the findings from the two parts of our case study of ArchiFirm to explore whether and in what ways our RDM overcame the limitations of traditional approaches to asset identification that we identify in Section X. We argue that the RDM brings significant benefits and does offer improvements for all three of these limitations.

5.1 A Finer Grain of Information Asset Identification

The first limitation concerns the coarse grain of asset identification in traditional ISRAs. Following the steps of OCTAVE-S, the risk analysis team at ArchiFirm (Table 1) identified a set of significant information assets (see Table 2). The method focused the team on infrastructural elements, which they described as “applications” and “systems”. However, when compared with the outputs of our RDM (see Table 4), the assets identified through OCTAVE-S were, as expected, at a very coarse level of granularity. In comparison, the infrastructural assets that we identified through the RDM were consistent with those that OCTAVE-S produced but had a greater range. By adopting an operational process perspective, through the BPMN-based rich process maps, the RDM made finer infrastructural distinctions between components such as the organization’s Web system, job-booking system, database system, backups, and desktops.

Similarly, the RDM identified conceptual information assets that the traditional ISRA overlooked. Using rich process maps and rich process narratives led to our identifying significant day-to-day operational resources, such as the soil and drafting templates, soil testing data, accounting scripts, and accounting data. This finer level of granularity that the RDM enabled provided a stronger basis to subsequently identify risks and to establish risk profiles around each asset. To confirm our general observation that our RDM produced a finer-grained analysis, Appendix A overviews the information assets that the RDM discovered and shows how many OCTAVE-S did not explicitly identify. One might argue that an ISRA does not need to identify assets in such detail because one can adequately assess their associated risks and treat them as part of larger-scale entities. However, there is a danger that by failing to make the component assets explicit, OCTAVE-S becomes a blunt tool for pinpointing specific risks and recommending later controls.

Importantly, with its ability to identify information containers and categories at a finer granularity, RDM points to the risks that an organization will lose data to uncontrolled containers and external parties. The rich process maps and rich process narratives provided useful resources to evaluate such risks relating to key data and information by considering their sensitivity from a confidentiality perspective and their exposure to possible leakage when at rest, in transit, and in use. That is, these techniques helped the analyst to reason about whether any unauthorized parties had access to information repositories (data at rest), if information flowed to authorized recipients in a secure manner (data in transit), and if data was being used in a secure manner (data in use). These lines of analysis promise to inform future decisions about the adequacy of current technical and non-technical security controls, which in turn will influence choices of targeted investment and improvements in security controls.

5.2 Broader Coverage of Information Assets to Encompass Informal Business Practices

The second limitation of current ISRAs concerns their breadth of coverage and, in particular, their focus on the formal aspects of the organization at the neglect of informal business practices. A part of OCTAVE-S that we conducted but do not report on here is its "vulnerability assessment", which places each critical information asset in an IT infrastructural context. Through predefined lists and diagrams and tables, this vulnerability assessment identified systems, people, and hardware linked to each information asset. However, despite tracing all of the connections between information and containers, the OCTAVE-S methodology identified no possibilities for information leakage. The method specifically asked the ArchiFirm risk analysis team for the *official storage locations* for each information asset with the question “Where would you go to get an *official* copy of the asset?”. However, the use of the word “official” in this question did not prompt them to consider the possibility that there might be a residue of *unofficial* copies produced as a by-product of the business process and left on various non-secure containers such as personal laptops, discarded print-outs, email attachments, and so on. In general, the manner in which OCTAVE-S framed its analysis of information assets did not promote consideration of the informal aspects of surrounding business practices.

In contrast, the RDM deliberately traced organizational workflows “on the ground” to examine how ArchiFirm conducted its work in practice, including workarounds and temporary holdings of information. As we intended, the rich process maps and rich process narratives captured both formal activities, such as staff’s copying information assets into folders and onto the servers, and informal activities, such as staff in the soils department’s copying, scanning, and communicating assets to external work environments. As we have noted already, such informal activities bring new risks that became apparent through the RDM. One example concerned the creation of personal and informal backups of company data. Given the frequency with which staff accidentally deleted or inadvertently overwrote files, these backups were clearly valuable in ensuring individuals could continually access critical data. However, as the analysis documented, an IT partner created and informally stored backups on BYODs on an office desk, in a car, and at a place of residence. This situation presented a range of possible threats to confidentiality because the various back-up locations were not easily protectable from a host of interception-based security risks. Looking beyond our case-study, one can clearly see this kind of trade-off between availability and confidentiality that arises through informal work practices in the recent trend of organizations’ adopting a bring-your-own-device (BYOD) policy. Such policies increase the range and severity of risks because unofficial copies of assets can proliferate on mobile devices. While security analysts and office managers now widely recognized the existence of this kind of risk, similar risks around informal business practices are not so easily identified. Our RDM provides a promising approach to discovering them.

5.3 The Identification of Knowledge Assets

The third area of limitation concerns whether and how the organization recognizes organizational knowledge as an asset that it needs to protect. Although members of the OCTAVE-S risk analysis team identified important people in ArchiFirm, they did not specify categories of organizational knowledge and their importance. In comparison, the techniques of the RDM guided the analysis towards the various elements of critical knowledge directly related to work tasks. ArchiFirm saw these elements as necessary to complete its work and for its competitiveness in its business environment.

OCTAVE-S focused the risk analysis team on examining people in the organization from an availability perspective. Its structured questions and templates did elicit responses about the general skills that a department brought to the organization, which did occasionally involve the label "knowledge". For example, the risk analysis team identified the IT team as critical for the organization’s information systems. They reasoned, as documented in their report, that the IT developer and IT-engineering partner held “particular knowledge and experience in the area” of IT and understood “programming, processes and workflows, hardware, applications and environment knowledge in IT”. But these observations did not specify the many essential practice-based elements of knowledge that were identified under the RDM, such as how to use applications, perform checks, or produce drafts conforming to clients’ requirements.

OCTAVE-S’s focus on key people and their availability, as opposed to a richer view of knowledge assets, limits the kind of threats that can be identified to loss of service and consequent harm to reputation, finances, productivity, and personnel safety. OCTAVE-S treats these "people" risks through security training, security management, and contingency planning initiatives. The ArchiFirm analysis team grew frustrated with the OCTAVE-S method when determining a mitigation approach for a “people” asset. The team members commented that they could not understand how a change in the “contingency planning” mitigation area would reduce the risk of a person’s being absent beyond having the other IT-related person present or contactable.

In contrast, the interviews that we conducted under our RDM included questions designed to elicit categories of organizational knowledge, to determine who held the knowledge, and what the security requirements were. Through the rich process maps and rich process narratives, we probed tacit forms of knowledge (e.g., Hislop, 2009) that were only describable indirectly in relation to one’s ability to conduct certain tasks or engage in certain practices effectively.

For example, consider the “client requirements drafting knowledge” category that the drafters and the head drafter held. This category clearly includes explicit knowledge about the standard procedures, rules, and templates for drafting. But, to perform their work efficiently and effectively, the drafters hold rich tacit knowledge about the particular needs and desires of particular clients and client groups. Drafters gain this tacit knowledge through the experience of working on reports for these clients and may learn it via socializing with other drafters. If ArchiFirm lost access to this tacit knowledge, it might still produce its drafts, but the product would be of a lower quality, which would likely threaten its competitiveness. Also

relevant here, and in need of protection, are the mechanisms for cultivating and maintaining this critical knowledge, such as the acts of work-based socialization between drafters.

Our RDM further identified difficult trade-offs in how ArchiFirm handled its knowledge assets. For example, the trade-off between availability and confidentiality; in other words, the dilemma between sharing knowledge in the firm and potentially leaking it to rivals. An interesting instance of this issue concerned junior engineers who often moved to ArchiFirm's rival firms to advance their careers. One might consider it detrimental to ArchiFirm's long-term competitiveness to share too much process knowledge with individuals who were likely to leave. A different issue was that, when analysis exposed the vulnerability of a single individual's holding vital knowledge, ArchiFirm often found it difficult to find a way to share the knowledge more widely. For example, the RDM pointed to the fact that one key individual, the office manager, held the knowledge about an important administrative area (i.e., how to manage the flow of work through ArchiFirm's main business processes). ArchiFirm had made attempts to share this knowledge with another administrator prior to the office manager's taking a lengthy period of leave but without success. In only two months of the office manager's absence, ArchiFirm experienced significant productivity problems without the "know-how" to avoid process bottlenecks.

6 Discussion

In our case study, we explored whether a richer analysis of an organization's information security assets could address limitations in current ISRAs as used in the security industry. The rich description method (RDM) that we devised and evaluated in the study combined techniques from qualitative field research and systems analysis methodologies, including semi-structured interviews, richly annotated business process modelling notation workflows, and scenario writing. Overall, we found that, when applying both our novel RDM and the traditional OCTAVE-S to the same organization, the RDM uncovered a greater range and depth of information security assets that needed protection. Specifically, we demonstrate that our RDM shows promise in addressing three key limitations of traditional ISRAs: the coarse granularity of assets identified, the narrow scope of assets that focuses overly on the official view of the organization, and the lack of attention to knowledge as an important asset type. We now consider both the practical and theoretical implications of these findings.

On the practical implications for industry practices of ISRA, two important qualifications must be made about these findings. First, while OCTAVE-S is a self-directed method that an organization's own staff can apply, our RDM is not fully developed in this way and our study required the lead author to apply it as an analyst. This fact complicates our comparison of the two approaches because they could not be applied in exactly the same way. To remedy this imbalance, our lead author was present when ArchiFirm administered both OCTAVE-S and the RDM. For the former, the firm needed his guidance less because the method is self-explanatory; for the latter approach, his guidance was more instrumental in the procedure. As such, the analyst influenced how ArchiFirm identified its assets and, thus, potentially biased our results. Mindful of his ability to influence the findings, the lead author took care to let the findings follow from the demands of the techniques that the RDM involved, although the potential for bias remained a possibility. This imperfect design must be balanced against the advantage that our study was set in a live risk assessment context of an organization that was genuinely motivated to identify its assets for protection.

Second, one might argue that the RDM produced a more detailed analysis, including of informal and knowledge aspects, simply because it spent more time collecting data than did OCTAVE-S. As Tables 1 and 3 show, applying RDM required a greater amount of total time (about 20 hours) and demanded the involvement of more staff compared to the time spent applying OCTAVE-S (about 14 hours). However, given that the OCTAVE-S workshops involved all three senior staff, their total effort (42 person hours) was greater than that for RDM's one-to-one interviews (20 person-hours). Nevertheless, the greater numbers of interviews under the RDM required more effort by the analyst team, and we found the interviews to be around 1.5 to two times longer than the time spent on the OCTAVE-S workshops in part because it took more time to gather details to construct process flows and write narratives than it did to answer OCTAVE-S's structured questions. Further, the RDM requires much additional work beyond the interviews to construct and finalize the rich process maps and rich process narratives. Further, note that applying the RDM to more complex processes than those we reviewed in studying ArchiFirm, with greater involvement of different organizational units and staff, would likely require increasing time and effort to organize and carry out.

However, when reflecting on the experience of applying the RDM and OCTAVE-S, we conclude that it was not through brute force of extra time or resources that the RDM produced its extended view of assets that ArchiFirm needed to protect. Rather, the richer responses it elicited resulted from a different perspective inherent in the data-collection mechanisms. OCTAVE-S's structured templates and worksheets oriented the risk analysis team toward the most tangible and easily identifiable assets, which tend to be the first answers that come mind in a group workshop when staff are asked to complete the fields of a structured template. However, behind them lurk other answers that staff might have provided through different forms of questioning and more imaginative scrutiny of the nature of organizational work. When conducting the RDM, the need to obtain the right kind of information to construct complete process models and complete narratives continually placed different demands on the interviewees. Questions probed the unmentioned and informal regions of work. For example, to probe the range of information assets, likely questions were: "Are there any assets the system users have created to assist in their work?", "What information is contained in these personally derived assets?", and even the more direct "Where would you go to receive unofficial copies of this information or data?". Therefore, practically speaking, the two approaches differed mainly due to the RDM's leading more naturally to open-ended reflection that exposed both the formal and informal aspects of the business processes under review. On this basis, we contend that the approach that the RDM adopts is a fruitful and practical direction for industry ISRA methodologies to explore.

Turning to more theoretical implications, we conducted our case study to explore a new business practice perspective on information security in line with other challenges to traditional perspectives (Dhillon & Backhouse, 2001). A practice perspective is reflected in RDM through the inclusion of techniques to develop rich accounts of organizational activity, rather than structured data, to guide the identification of assets. A commitment to practice is also reflected in the approach of interviewing a broad range of staff, including those working within the processes under review, rather than the more narrow focus in OCTAVE-S on small teams of managers.

One consequence of the practice perspective that underlies our RDM is to shift security theorizing away from a purely information technology focus (Dhillon & Backhouse, 2001; Guo, 2010; Siponen, 2005b; Zafar & Clark, 2009). Technology vulnerabilities and attacks remain a source of major concern and loss for organizations and a productive area of research. However, by probing the "actual" way that staff complete work, the RDM's techniques facilitate analysts to examine not only the role of information technology but also the role of surrounding social interactions and a wide range of unofficial information artifacts, including paper-print outs, memory sticks, and so on.

In our report of the findings, we observed how the RDM reveals a greater breadth of information assets. But there is a deeper point to be made here about the way traditional approaches favor a form of abstraction in analysis that reflects the traditional technical systems perspective. That is, traditional approaches seek to identify general classes of informational assets. In contrast, a practice perspective focuses more on reality than formal abstraction, and, hence, our RDM made important distinctions between the different instances (or copies) of the same information asset. A practice perspective recognizes that individuals frequently create temporary copies on the fly as part of routine work, whereas a traditional ISRA methodology focuses on high-level asset categories and official copies. Hence, a practice-based approach exposes the existence of informally created assets that are frequently not subject to the same security protocols, which manifests a different layer of information security risks.

The practice perspective confronts rather than denies the organization's informal side. As a result, among other things, it provides a stronger basis to observe and combat the leakage of business critical information into the wrong hands. The traditional concept of one static "official" copy of an information asset is often naïve. Instead, in practice, one should conceptualize information as a living entity. Unseen informal work practices often involve dissecting information into different fragments, copying fragments of collections of information between multiple devices, transmitting information to other parties, and transferring information across "containers". In such a conceptualization, the possibilities for information leakage are multiple and various. We need to understand this complex, practical life of information. Future ISRA methods should establish an understanding that organizational information is not limited to "official" copies (Alberts et al., 2003; Bernard, 2007). We found the business process and narrative techniques in our RDM to expose at least some of the vulnerabilities of information leakage and to identify specific incidents of critical and sensitive information's being copied or shifted to unofficial information containers.

Further, the practice perspective as explored in our case study points to the need for a stronger connection between information security and the knowledge management field (e.g., Hislop, 2009).

Security research has largely ignored knowledge (and the practices around cultivating and sharing it) as an area worth investigating (Gold & Arvind Malhotra, 2001). The observation that knowledge is a valuable asset is not controversial, but our study illustrates that we need a shift in security perspective to appropriately reflect knowledge as an asset that one needs to protect. We need a fundamental shift away from the view that sees individuals as the assets towards one that acknowledges classes of knowledge as the assets. Different people may or may not possess classes of knowledge assets. If a person holds critical knowledge, firms can scrutinize knowledge management practices such as socialization and codification (Nonaka & Toyama, 2003) for the risks they raise to confidentiality, and, further, firms may regard them as potential security controls for threats to availability in other situations (Hansen, Nohria, & Tierney, 1999).

7 Conclusions, Limitations, and Future Research

In this paper, we argue and demonstrate that traditional structured ISRAs have limitations in the way they conceptualize and identify organizations' information assets that they need to protect. We present an alternative approach called the rich description method (RDM) (which we developed based on inspiration from ethnography's "thick" descriptions), to help firms achieve a richer account of both their formal and informal aspects. The comparative results of applying a traditional ISRA and the RDM to the same company showed that the RDM identified a wider range and depth of information assets and could better identify organizational knowledge as an asset. As we argue throughout the paper, the RDM provided a more nuanced view that was potentially more informative when considering important vulnerabilities, such as possibilities for leaking sensitive information and competitive knowledge to rivals.

We devised the RDM as a research vehicle to explore richer possibilities for collecting data and analyzing information security. We do not intend it as a fully formed or validated ISRA method. We do not present the RDM, therefore, as replacing traditional ISRAs. Rather, we claim that its use in our study demonstrates that richer data-collection and analysis techniques are available and promising and that, when used in conjunction with well-formed methods such as OCTAVE-S, they offer to extend the range of security assessments. Whether such techniques are valuable in practice depends on their cost-benefit ratio in particular circumstances. Of course, organizations might choose to use different methods for different part of their work; for example, they might choose to apply more probing RDM-style techniques only to their mission-critical organizational processes as was the case for the organization we studied in this paper. Another circumstance affecting the value of RDM in practice is whether the targeted processes are relatively stable or continuously changing. A detailed RDM-style investigation is probably most valuable for business processes that are complex but relatively stable such that the one-off cost would support future security controls for a longer term.

We need further research to extend the current investigation by exploring other rich data-analysis techniques to chart the assets, vulnerabilities, and risks associated with organizations' informal side. We also need to better understand the methodological context in which such techniques are applied. For example, it would be valuable to establish whether one could devise a self-directed form of the current RDM such that organizations could apply it by themselves with the same efficacy as we achieved in this study.

In conclusion, we offer our RDM as a potential pathway for researchers to develop richer alternative information security risk methodologies. Our findings suggest that methods oriented towards business practices (and, thus, that encompass both formal and informal practices and that are sensitive to the risks of leaking knowledge about critical business processes to rivals) have great value. We argue that approaches such as the RDM are especially relevant for knowledge-intensive organizations where information and expertise constitute their primary competitive assets.

References

Ahmad, A., Bosua, R., & Scheepers, R. (2014a). Protecting organizational competitive advantage: A knowledge leakage perspective. *Computers & Security*, *42*, 27-39.

Ahmad, A., Maynard S., & Park, S. (2014b). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*. *25(*2). 357-370.

Ahmad, A., Ruighaver, A. B., & Teo, W. T. (2005). An information-centric approach to data security in organizations. In *Proceedings of IEEE TENCON*. (pp. 1-5).

Alberts, C. J., & Dorofee, A. (2002). *Managing information security risks: The OCTAVE approach.* Boston: Addison-Wesley Longman.

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2003). *Introduction to the OCTAVE approach*. Pittsburgh, PA, Carnegie Mellon University.

Bass, T., & Robichaux, R. (2001). Defense-in-depth revisited: Qualitative risk analysis methodology for complex network-centric operations. In *Proceedings of the Military Communications Conference* (pp. 64-70). IEEE.

Bernard, R. (2007). Information lifecycle security risk assessment: A tool for closing security gaps. *Computers & Security*, *26*(1), pp. 26-30.

Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. In *Proceedings of the 2001 Workshop on New Security Paradigms* (pp. 97-104). ACM.

Brown, J. S., & Duguid, P. (2002). *The social life of information*. Boston, MA: Harvard Business Press.

Checkland, P. (2000). Soft systems methodology: A thirty year retrospective. *Systems Research and Behavioral Science*, *17*, S11-S58.

Cook, S. D., & Brown, J. S. (1999). Bridging epistemologies: The generative dance between organizational knowledge and organizational knowing. *Organization Science*, *10*(4), 381-400.

Cooper, L. F. & Johnson, A. (2003). *Security risk management: Strategies for managing vulnerabilities and threats to critical digital assets.* Washington, DC: CRA Reports.

Darke, P., Shanks, G., & Broadbent, M. (1998). Successfully completing case study research: Combining rigour, relevance and pragmatism. *Information Systems Journal*, *8*(4), 273-289.

Davenport, T. H., & Prusak, L. (1998). *Working knowledge: How organizations manage what they know.* Boston, MA: Harvard Business Press.

den Braber, F., Hogganvik, I., Lund, M. S., Stølen, K., & Vraalsen, F. (2007). Model-based security analysis in seven steps—a guided tour to the CORAS method. *BT Technology Journal*, *25*(1), 101-117.

Dhillon, G. (2007). *Principles of information systems security: Text and cases* (pp. 97-129). New York, NY: Wiley.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal*, *11*(2), 127-153.

Dubé, L., & Paré, G. (2003). Rigor in information systems positivist case research: Current practices, trends, and recommendations. *MIS Quarterly*, *27*(4), 597-636.

Dumas, M., La Rosa, M., Mendling, J., & Reijers, H. A. (2013). *Fundamentals of business process management* (pp. I-XXVII). Berlin: Springer.

Eloff, J. H. P., & Eloff, M. M. (2005). Information security architecture. *Computer Fraud & Security*, *2005*(11), 10-16.

Farahmand, F., Navathe, S. B., Enslow, P. H., & Sharp, G. P. (2003). Managing vulnerabilities of information systems to security incidents. In *Proceedings of the 5th International Conference on Electronic Commerce* (pp. 348-354). ACM.

Farris, G. F. (1979). The informal organization in strategic decision-making. *International Studies of Management & Organization*, *9*(4), 37-62.

Frosdick, S. (1997). The techniques of risk analysis are insufficient in themselves. *Disaster Prevention and Management: An International Journal*, *6*(3), 165-177.

Geertz, C. (1994). Thick description: Toward an interpretive theory of culture. In M. Martin & L. McIntyre (Eds.), *Readings in the philosophy of science* (pp. 213-231). Cambridge, MA: MIT Press.

Gerber, M., & Von Solms, R. (2001). From risk analysis to security requirements. *Computers & Security, 20*(7), 577-584.

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

Gherardi, S. (2000). Practice-based theorizing on learning and knowing in organizations. *Organization-London*, *7*(2), 211-224.

Gold, A. H., & Arvind Malhotra, A. H. S. (2001). Knowledge management: An organizational capabilities perspective. *Journal of Management Information Systems*, *18*(1), 185-214.

Guo, K. H. (2010). Knowledge for managing information systems security: Review and future research directions. In E. M. Alkhalifa (Ed.), *E-strategies for resource management systems: Planning and implementation* (pp. 266-286). Hershey, PA: Business Science Reference.

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

Hamilton, C. R. (1998). *New trends in risk management.* Auerbach.

Hansen, M. T., Nohria, N., & Tierney, T. (1999). What's your strategy for managing knowledge? *Harvard Business Review*, *77*(2), 106-116.

Hislop, D. (2009). *Knowledge management in organizations*. New York: Oxford University Press**.**

ISO/IEC. (2001). *17799 code of practice for information security management.*

Jones, A., & Ashenden, D. (2005). *Risk management for computer security: Protecting your network & information assets.* Newton, MA: Butterworth-Heinemann.

Jung, C., Han, I., & Suh, B. (1999). Risk analysis for electronic commerce using case-based reasoning. *International Journal of Intelligent Systems in Accounting, Finance & Management*, *8*(1), 61-73.

Kokolakis, S. A., Demopoulos, A. J., & Kiountouzis, E. A. (2000). The use of business process modelling in information systems security analysis and design. *Information Management & Computer Security*, *8*(3), 107-116.

Landoll, D. J., & Landoll, D. (2005). *The security risk assessment handbook: A complete guide for performing security risk assessments.* Boca Raton, FL: CRC Press.

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

Lim, J. S., Ahmad, A., Chang, S., & Maynard, S. B. (2010). Embedding information security culture emerging concerns and challenges. In *Proceedings of the Americas Conference on Information Systems.*

McFadzean, E. (1998). Enhancing creative thinking within organisations. *Management Decision*, *36*(5), 309-315.

Moody, D. L., & Walsh, P. (1999). Measuring the value of information-an asset valuation approach. In *Proceedings of the European Conference on Information Systems* (pp. 496-512).

Nadler, D. A., & Tushman, M. L. (1980). A model for diagnosing organizational behavior. *Organizational Dynamics*, *9*(2), 35-51.

Nonaka, I. (1991). The knowledge-creating company. *Harvard Business Review*, *69*(6), 96-104.

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

Nonaka, I., & Toyama, R. (2003). The knowledge-creating theory revisited: Knowledge creation as a synthesizing process. *Knowledge Management Research & Practice*, *1*(1), 2-10.

Peltier, T. R. (2001). *Information security risk analysis*. Boca Raton, FL: CRC Press.

Qayoumi, M. H., & Woody, C. (2005). Addressing information security risk. *Educause Quarterly*, *28*(4), 7-11.

Reid, R. C., & Floyd, S. A. (2001). Extending the risk analysis model to include market-insurance. *Computers & Security*, *20*(4), 331-339.

Röhrig, S., & Knorr, K. (2004). Security analysis of electronic business processes. *Electronic Commerce Research*, *4*(1-2), 59-81.

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

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

Sasse, M. A., & Flechais, I. (2005). Usable security: Why do we need it? How do we get it? In. L. F. Cranor & S. Garfinkel (Eds.), *Security and usability: Designing secure systems that people can use* (pp. 13-30). Sebastopol: O'Reilly Media.

Satchidananda, S. S., & Shanthamurthy, D. (2004). *Implementing information security in banks.* Bangalore: Indian Institute of Technology.

Seddon, P. B., & Scheepers, R. (2012). Towards the improved treatment of generalization of knowledge claims in IS research: Drawing general conclusions from samples. *European Journal of Information Systems*, *21*(1), 6-21.

Shedden, P., Ruighaver, A. B., & Ahmad, A. (2010). Risk management standards—the perception of ease of use. *Journal of Information Systems Security, 6*(3). 23-41.

Shedden, P., Scheepers, R., Smith, W., & Ahmad, A. (2011). Incorporating a knowledge perspective into security risk assessments. *Vine*, *41*(2), 152-166.

Shedden, P., Smith, W., Scheepers, R., & Ahmad, A. (2009). Towards a knowledge perspective in information security risk assessments—an illustrative case study. In *Proceedings of the 20th Australasian Conference on Information Systems (pp. 74-84).* Melbourne, Australia: Monash University.

Shedden, P., Smith, W., Ahmad, A. (2010). Information security risk assessment: Towards a business practice perspective. In *Proceedings of the 8th Information Security Management Conference* (pp. 127-138).

Siponen, M. T. (2005a). Analysis of modern IS security development approaches: Towards the next generation of social and adaptable ISS methods. *Information and Organization, 15*(4), 339-375.

Siponen, M. T. (2005b). An *analysis of the traditional IS security approaches: Implications for research and practice. European Journal of Information Systems*, *14*(3), 303-315.

Slay, J., & A. Koronios (2006). Information technology security & risk management. Milton, QLD: Wiley.

Spears, J. L. (2006). A holistic risk analysis method for identifying information security risks. In P. Dowland, S. Furnell, B. Thuraisingham, & X. S. Wang (Eds.), *Security management, integrity, and internal control in information systems* (pp. 185-202). New York: Springer.

Spinellis, D., Kokolakis, S., & Gritzalis, S. (1999). Security requirements, risks and recommendations for small enterprise and home-office environments. *Information Management & Computer Security*, *7*(3), 121-128.

Stacey, T. R., Helsley, R. E., & Baston, J. V. (1996). Identifying information security threats. *Information Systems Security*, *5*(3), 50-59.

Standards Australia. (2004a). *HB 231. Information security risk management guidelines.*

Standards Australia. (2004b). *AS/NZS 4360. Risk management*.

Stølen, K., den Braber, F., Dimitrakos, T., Fredriksen, R., Gran, B. A., Houmb, S. H., Lund, M. S., Stamatiou, Y., & Aagedal, J. O. (2002). Model-based risk assessment—the CORAS approach. In *Proceedings of the iTrust Workshop*.

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). *Sp 800-30. Risk management guide for information technology systems.* Gaithersburg, MD: National Institute of Standards & Technology.

Tsoukas, H. (1996). The firm as a distributed knowledge system: A constructionist approach. *Strategic Management Journal*, *17*, 11-25.

Venters, W., Cushman, M., & Cornford, T. (2003). *Creating knowledge for sustainability: Using SSM for describing knowledge environments and conceptualising technological interventions*. London, UK: London School of Economics and Political Science.

Visintine, V. (2003). *An introduction to information risk assessment.* SANS institute.

Warren, M., & Hutchinson, W. (2003). A security risk management approach for e-commerce. Information Management & Computer Security, *11*(5), 238-242.

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security*, *44*, 1-15.

West, S., & Andrews, A. D. (2003). *OCTAVE—best practices comparative analysis* (ATI IPT Technical Report, 03-4).

West, S., Crane, L. S., & Andres, A. D. (2002). *OCTAVE-DITSCAP comparative analysis*. Fort Detrick, Fredrick: US Army Medical Research and Material Command.

Whitman, M., & Mattord, H. (2014). *Principles of information security.* New York: Cengage Learning.

Wood, L. E. (1997). Semi-structured interviewing for user-centered design. *Interactions*, *4*(2), 48-61.

Yazar, Z. (2002). *A qualitative risk analysis and management tool—CRAMM* (SANS InfoSec reading room white paper).

Yin, R. (2009). *Case study research: Design and methods*. Newbury, CA: Sage.

Zafar, H., & Clark, J. G. (2009). Current state of information security research in IS. *Communications of the Association for Information Systems*, *24*, 557-596.

Appendix A: Comparison of Information and Knowledge Assets Identified between RDM and OCTAVE-S

Table A1. Comparison of Assets Identified Between the RDM and OCTAVE-S

RDM information assets identified	OCTAVE-S equivalent
Soils faxed order forms	Job information and/or job booking system
Soils delivered order	Job Information and/or job booking system
Photographs	**Not identified** (Implicit under "job information", though contextual discussion showed that job information related to orders forms)
Soil report	Drafts/final documentation (Implicit under "soils and survey system")
Soil report templates	**Not identified**
Arch. drawings	Job information
Drafts	Drafts/final documentation
Engineered drafts	Drafts/final documentation
Checked engineered drafts	Drafts/final documentation
CadeComp	Engineering software
Eng. Excel templates	Engineering software
Accounting spreadsheets	**Not identified** (Implicit under "accounting system")
Accounting scripts	**Not identified** (Implicit under "accounting system")
Handy backup	**Not identified** (Implicit under "accounting system")
Accounting data	**Not identified** (Implicit under "accounting system")
Database	**Not identified** (Implicit under "database system", though not specifically identified and established under the methodology)
Database system	Database system
Soil test job allocation knowledge	**Not identified** (No OCTAVE-S identified equivalent)
Soil report checking knowledge	Soils
Drafting job allocation knowledge	**Not identified** (No OCTAVE-S identified equivalent)
Client requirements drafting knowledge	**Not identified** (Drafting as a people-category asset does not include knowledge of client requirements)
Client requirements engineering knowledge	**Not identified** (The "principals/partners" people-category asset is the closest, but it referred to the partners' ability to communicate with clients, and not to the critical knowledge of checking)
Client-specific engineering checking knowledge	**Not identified** (The "principals/partners" people-category asset is the closest, but it referred to the partners' ability to communicate with clients, not to the critical knowledge of checking.)

Table A1. Comparison of Assets Identified Between the RDM and OCTAVE-S

Process management knowledge	**Not identified** (The “administration” people-category asset related more to tasks that the person performed, not to their knowledge of the organization)
Database maintenance knowledge	**Not identified** (The “IT department” people-category asset related more to the skills of the IT developer and his ability to code and deploy hardware, not necessarily to his knowledge of the database's operations and construction)
Accounting script knowledge	**Not identified** (Could be implicit under “accounts”, but this description of the people-asset category related more to the official knowledge of QuickBooks)
Accounts checking knowledge	**Not identified** (Discussion around “accounts” as a people-asset category did not relate to the checking processes that occurred to ensure that orders were entered appropriately)

About the Authors

Piya Shedden is a Client Manager in the Cyber Risk Advisory service line of Deloitte Australia. He is an expert in Information Security with an emphasis on Risk and Privacy. He completed his PhD and Bachelor degrees at the University of Melbourne. His research interests include the study of information security risk management methods and the exploration of holistic and social perspectives of security risk, incorporating practice perspectives and knowledge security.

Atif Ahmad is an academic based at the Department of Computing and Information Systems, University of Melbourne. His research interests are in the management of information security in organizations specifically relating to strategy, risk, culture, and incident response. In previous years, he worked as a consultant for Pinkerton and WorleyParsons where he applied his expertise to Internet corporations and critical infrastructure installations. He is a Board Certified Protection Professional (CPP) with the American Society for Industrial Security and holds an adjunct position at the SecAU Security Research Centre at Edith Cowan University.

Wally Smith is a Senior Lecturer in the Department of Computing and Information Systems at the University of Melbourne. He conducts research into the design of usable digital technologies in the domains of health, education and public history. Recent and ongoing projects include *New Tools and Techniques for Learning in the Field* (Office for Learning and Teaching), *Social Network Sites for Ambivalent Socialisers: The Case of Smoking Cessation* (Australian Research Council), and *Citizen Heritage: Digital and Community-based Histories of Place* (Australian Research Council).

Heidi Tscherning is an academic based in the Department of Information Systems and Business Analytics, Deakin University. Her current research focus is in the area of value creation based on analytics investments, and consequences for consumers as well as organizations; in particular consumer privacy and organizational knowledge protection. She also researches how individual social contexts influence the adoption and use of ubiquitous technologies. She holds a PhD from Copenhagen Business School. Prior to working in academia, she worked as an IT project manager and IT management consultant in industries, such as IT, pharmaceuticals, and national defence.

Rens Scheepers currently serves as Head of Department in the School of Information Systems and Business Analytics in the Faculty of Business and Law at Deakin University in Victoria, Australia. He has conducted research on topics such as knowledge strategy, and the role of information technology in competitive advantage generation. His publications have appeared in highly-ranked journals in the Information Systems discipline, including the *European Journal of Information Systems*, *Journal of Information Technology*, *Information Systems Journal* and *Journal of the Association of Information Systems*. He currently serves on the editorial boards of the *Journal of Information Technology,* and the *Journal of Strategic Information Systems*.