JITTA

JOURNAL OF INFORMATION TECHNOLOGY THEORY AND APPLICATION

ISSN: 1532-3416

Foundations for an Intelligence-driven Information Security Risk-management System

Jeb Webb
Department of Computing and Information Systems, University of Melbourne, Australia
jeb.webb@unimelb.edu.au

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

Sean B. Maynard
Department of Computing and Information Systems, University of Melbourne, Australia
sean.maynard@unimelb.edu.au

Graeme Shanks
Department of Computing and Information Systems, University of Melbourne, Australia
gshanks@unimelb.edu.au

Abstract:

Information security risk management (ISRM) methods aim to protect organizational information infrastructure from a range of security threats by using the most effective and cost-efficient means. We reviewed the literature and found three common deficiencies in ISRM practice: 1) information security risk identification is commonly perfunctory, 2) information security risks are commonly estimated with little reference to the organization's actual situation, and 3) information security risk assessment is commonly performed on an intermittent, non-historical basis. These deficiencies indicate that, despite implementing ISRM best-practice, organizations are likely to have inadequate situation awareness (SA) regarding their information security risk environments. This paper presents a management system design that organizations can use to support SA in their ISRM efforts.

Keywords: Information Security, Risk Management, Risk Assessment, Situation Awareness, Intelligence (Collection and Analysis), Monitoring.

Wendy Hui was the the Senior Editor for this paper.

1 Introduction

Best practice information security standards, such as the ISO/IEC 27000 series, advise organizations to use a risk-management approach to reduce risk exposure to acceptable levels. A risk-management approach requires that one ranks and prioritize assets' security risks after which one can employ risk-treatment strategies to manage the risks associated with these assets (ISO 31000:2009, 2009). The success of the information security risk management (ISRM) process hinges on accurately assessing the organization's information security risk environment.

In reviewing the literature, we did not identify any studies that make generalized claims about the effectiveness of information security risk assessments in organizations (Webb, Ahmad, Maynard, & Shanks, 2014). Two likely reasons explain this omission: 1) the sensitive nature of the topic makes it difficult to find organizations that will agree to participate in such research and 2) it requires in-depth knowledge of both information security and risk management methods.

However, we identified three key deficiencies among the considerable scholarly criticism (in the light of findings from many in-depth case studies) of the ways in which many organizations assess information security risk (which we summarize in Section 2.1). These deficiencies in risk assessment are tantamount to situation awareness (SA) deficiencies because they describe ways in which practitioners fail to perceive, comprehend, or make reliable projections about information security risk (Webb et al., 2014). Where SA is deficient, managers cannot accurately determine asset vulnerabilities, how exploits might exploit vulnerabilities, and how to best defend these assets in the most cost-effective manner possible. Accordingly, the following question guides our research: "How can situation awareness be improved in information security risk management?".

In this theory-building paper, we build on Endsley's (1988) situation awareness theory to propose a comprehensive answer to the above question. The solution we offer is a design science artifact: a risk management system[1] that organizations can implement to maximize SA in ISRM. The intelligence-driven information security risk management system (ID-ISRMS) is an organizational system design based on the U.S. national security intelligence enterprise (USNSIE) model. It aims to increase SA in ISRM via a permanent intelligence cycle.

The paper proceeds as follows: in Section 2, we provide background information on ISRM and present practical deficiencies we identified when reviewing the literature on SA theory. In Section 3, we explain SA theory and Endsley's (1995) theoretical model. In Section 4, we explain how we followed Peffers, Tuunanen, Rothenberger, and Chatterjee's (2007) design science research methodology to develop an artifact that might redress the identified deficiencies. We present the artifact in Section 5. In Section 6, we present findings from a focus group evaluation of the artifact. In Section 7, we discuss the results and, in Section 8, conclude the paper.

Contribution:

This paper contributes to information security risk management (ISRM) in several ways. It argues that three critical deficiencies exist in ISRM and that one can address them by using Endsley's (1988) situation awareness (SA) theory. The paper develops an intelligence-driven information security risk management system (ID-ISRMS), a system based on the U.S. national security intelligence enterprise (USNSIE) model. The recommended ID-ISRMS design can increase SA via an intelligence cycle, which supports evidence-based (as opposed to "gut feel") decision making in ISRM. Designed to redress three major practical deficiencies identified in literature, this ID-ISRMS is an artifact that supports managerial decision making to improve the defensive posture of the implementing organization.

[1] A management system refers to "the set of procedures an organization needs to follow in order to meet its objectives" (see ISO, n.d.).

2 Background: Information Security Risk Management

Most industry standards endorse a risk-management approach to information security (e.g., those published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) or by the U.S. National Institute of Standards and Technology (NIST)). As such, practitioners have access to a plethora of "information security risk management" methods[2].

In this paper, we refer to the ISO/IEC 27005 (2011) standard as a best practice method. We chose ISO/IEC 27005 because of its international standing and widespread adoption across the developed world. Table 1 describes the ISRM process as ISO/IEC 27005 prescribes it.

Table 1. The ISO/IEC 27005 Framework

Context establishment		"The external and internal context for information security risk management should be established, which involves setting the basic criteria necessary for information security risk management, defining the scope and boundaries, and establishing an appropriate organization operating the information security risk management." (§7.1)
Risk assessment	**Risk identification**	**Asset identification:** "The assets within the established scope should be identified." (§8.2.2) **Threat identification:** "Threats and their sources should be identified." (§8.2.3) **Control identification:** "Existing and planned controls should be identified." (§8.2.4) **Vulnerability identification:** "Vulnerabilities that can be exploited by threats to cause harm to assets or to the organization should be identified." (§8.2.5) **Consequence identification:** "The consequences that losses of confidentiality, integrity and availability may have on the assets should be identified." (§8.2.6)
	Risk analysis	**Consequence assessment:** "The business impact upon the organization that might result from possible or actual information security incidents should be assessed, taking into account the consequences of a breach of information security such as loss of confidentiality, integrity or availability of the assets." (§8.3.2) **Incident likelihood assessment:** "The likelihood of the incident scenarios should be assessed." (§8.3.3) **Risk level determination:** "The level of risk should be determined for all relevant incident scenarios." (§8.3.4)
	Risk evaluation	"Level of risks should be compared against risk evaluation criteria and risk acceptance criteria." (§8.4)
Risk treatment		"Controls to reduce, retain, avoid, or share the risks should be selected and a risk treatment plan defined." (§9.1)
Risk acceptance		"The decision to accept risks and responsibility for the decision should be made and formally recorded." (§10)
Risk communication and consultation		"Information about risk should be exchanged and/or shared between the decision-maker and other stakeholders." (§11)
Risk monitoring and review		"Risks and their factors (i.e., value of assets, impacts, threats, vulnerabilities, likelihood of occurrence) should be monitored and reviewed to identify any changes in the context of the organization at an early stage, and to maintain an overview of the risk picture." (§12.1)

Whitman and Mattord (2012) explain that doing ISRM well requires examining all of an organization's information assets for vulnerability, scrutinizing the effectiveness of any control strategies it currently uses, and—to the greatest extent possible—assessing whatever threats to information security might face the organization.

Though standard methods entreat practitioners to approach ISRM as rigorously and holistically as possible, a body of research suggests many do not actually do so. We identified three common practical ISRM deficiencies in the literature.

2.1 Deficiency 1: Information Security Risk Identification is Commonly Perfunctory

Risk assessments are often simply not as rigorous as they need to be in order to reflect the reality of the situation (Baskerville, 1991; Parker, 2007; Utin, Utin, & Utin, 2008). Several authors have identified

[2] For a comprehensive list of ISRM methods, see (Enisa, n.d.).

significant sources of information security risk that are commonly overlooked during the risk identification phase of the risk-assessment process.

Examples include:

1. Threats and vulnerabilities associated with **intangible knowledge assets**, such as proprietary knowledge connected to competitive advantage or practical knowledge pertaining to the execution of critical business processes (Shedden, Scheepers, Smith, & Ahmad, 2011; Ahmad, Bosua, & Scheepers, 2014).
2. Threats and vulnerabilities associated with **complex asset interdependencies**, such as interdependency or indirect relationships between multiple technological information assets (Parker 2007; Utin et al., 2008; Nazareth & Choi 2015; Friedberg, Skopik, Settanni, & Fiedler, 2015).
3. Threats and vulnerabilities associated with **non-technological contextual factors,** such as organizational policies, procedures, or culture (Vroom & Von Solms, 2004; Al-Ahmad & Mohammad, 2012; Da Veiga & Eloff, 2010; Da Veiga & Martins, 2015; Flores, Antonsen, & Ekstedt, 2014; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014).
4. Threats and vulnerabilities associated with patterns of **employee behavior** (Kowalski, Cappelli, & Moore, 2008; Colwill, 2009; Stewart & Lacey, 2012; Guo, 2013; Crossler et al., 2013).
5. **Historical threats and vulnerabilities** that past incident reports identified but which the organization subsequently forgot about (Ahmad, Hadgkiss, & Ruighaver 2012) or that it never really analyzed after an incident (Ab Rahman, Hidayah, & Choo, 2015).
6. Threats and vulnerabilities associated with persistent attack or **strategizing threat agents** (Parker, 2007; Raiu, 2012; Baracaldo & Joshi, 2013; Fenz, Heurix, Neubauer, & Pechstein, 2014; Friedberg et al., 2015).

These kinds of omissions arise from the various problematic operational conditions in organizations. For example, the lack of rigor may owe to the fact that ISRM requires expertise in both information security and risk-management practices (Shedden, Ruighaver, & Atif, 2010). The absence of an information-sharing culture in organizations is another problematic operational condition (Shedden et al., 2011; Ahmad et al., 2012; Ahmad, Maynard, & Shanks, 2015). Further, there is a popular misapprehension that compliance with standards equals information security (Von Grebmer, 2007, p. 40; Siponen, 2006; Matwyshyn, 2009; Shedden et al., 2010; Al-Ahmad & Mohammad, 2012; Flores et al., 2014).

2.2 Deficiency 2: Information Security Risks are Commonly Estimated with Little Reference to the Organization's Actual Situation

Risk-assessment practices have been criticized for oversimplifying the information security risk environment and yielding non-representative, largely symbolic estimations of risk; practitioners often rely chiefly on inference in lieu of hard evidence (Baskerville, 1991; Parker, 2007; Utin et al., 2008). Collecting and analyzing all data required to diagnose the state of the risk environment is an inherently difficult task (Parker, 2007; Utin et al., 2008) that also requires a significant amount of intra-organizational cooperation and coordination (Coles & Moulton, 2003; Young & Windsor, 2010; Tøndel, Line, & Jaatun, 2014). Difficulties stem not only from the workload and logistics involved but also from the objective paucity of some kinds of data (perhaps most significantly, current threats) (Whitman & Mattord, 2012).

Gathering data about, for example, the greater risk environment (i.e., the organization's external context) is difficult because organizations generally choose not to discuss their information security practices (Kotulic & Clark, 2004; Crossler et al., 2013; Friedberg et al., 2015). Several researchers have noted that a lack of proactive information sharing between information security practitioners prevents them from developing an accurate common picture of the risk environment (Werlinger. Muldner, Hawkey, & Beznosov, 2010; Fang, Liang, & Jia, 2011; Fenz, 2012; Tamjidyamcholo & Al-Dabbagh, 2012; Feledi, Fenz, & Lechner, 2013; Tamjidyamcholo, Baba, Tamjid, & Gholipour, 2013; Tamjidyamcholo, Baba, Shuib, & Rohani, 2014).

Internally, many organizations also fail to recognize actual relationships between information asset security, whole information system security (people, processes, data, and technology), and business process security (Coles & Moulton, 2003; Baker, Rees, & Tippett, 2007; Fenz, Ekelhart, & Neubauer ,2009; Fenz et al., 2014; Nazareth & Choi, 2015), which results in information security risk assessments

that are somewhat dissociated from the bigger risk picture (i.e. how the risks to information assets translate to actual operational and strategic risks for the organization).

The common problem of vague or fragmentary information asset inventories (Shedden et al., 2016 Al-Ahmad & Mohammad, 2012) precludes one from comprehensively mapping individual assets' roles in business processes or from identifying specific linkages between the assets and broader strategic objectives. In the interest of symbiosis between information security and business operations, Coles and Moulton (2003) and Fenz et al. (2009) have recommend conducting ISRM specifically in the context of business processes—and requiring the direct participation of business process owners—to ensure that the organization fully understands the strategic business value of information assets.

2.3 Deficiency 3: Information Security Risk Assessment is Commonly Performed on an Intermittent, Non-historical Basis

Organizations typically conduct information security risk assessments somewhere between quarterly and annually (Rees & Allen, 2008); that organizations typically perform information security risk assessments at spaced cycles and in short timeframe can result in periods of critical inattention to the risk environment (Hulme, 2004; Rees & Allen, 2008; Schmittling, 2010; Crossler et al., 2013; Da Veiga & Martins, 2015). Such an approach is bound to result in significant temporal blind spots during which risk-related developments may arise and pass away unnoticed without ever informing managerial perceptions (or assessments) of risk (Hulme, 2004; Schmittling, 2010). These blind spots hamper the organization from identifying risks associated with strategizing threat agents or other historically recurrent threats (see Section 2.1), which, in turn, undermine risk analysis and evaluation efforts.

Infrequent risk assessments also create a paradoxical problem in which data overload occurs despite an actual dearth of relevant data. Practitioners must not only reorient themselves—along with any team members—to the current state of a dynamic risk environment that has no doubt changed since the last risk assessment (possibly due to unobserved causes that are now mysteries) but also manage and execute the new "assessment project" in a limited timeframe. Under these circumstances, less investigation would still mean less awareness, but even the most rigorous efforts might be confounded if some important things happened during preceding months while no one was looking.

When we add to these problems associated with intermittency the fact that poor recordkeeping and inadequate information sharing between stakeholders commonly hinders the organizational memory/knowledge required for skillfully interpreting the risk environment (Jaatun, Albrechtsen, Line, Tøndel, & Longva, 2009; Shedden et al., 2011; Ahmad et al., 2012; Tøndel et al., 2014; Rhee, Ryu, & Kim, 2012; Da Veiga & Martins, 2015; Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009; Flores et al., 2014; Parsons et al., 2014), the aggregate result is the omission of huge swaths of information from risk assessments.

The three deficiencies outlined above obscure what is really going on in the information security risk environment and, as such, ultimately constitute basic situation awareness problems. This reduced situation awareness has negative consequences for managerial decision making and action because unrealistic perceptions of risk can lead to inappropriate risk-treatment strategies (Rhee et al., 2012; Qian, Fang, & Gonzalez, 2012; Ahmad, Bosua, & Scheepers, 2014; Pfleeger & Caputo, 2012).

What the literature does not clearly explain is why exactly these practical deficiencies exist in organizations. We know that, in many cases, executive decision makers simply misapprehend the nature of information security risk or the amount of work that is actually involved in performing a realistic risk assessment (see Siponen, 2006; Shedden et al., 2010; Matwyshyn, 2009, for how this can be the case). These kinds of misapprehensions no doubt relate to fundamental problems with the way security practitioners popularly think about information security management. These problems include the predominance of reactive as opposed to proactive approaches (Qian et al., 2012) and myopically IT-centric views of information systems (Jaatun et al., 2009; Reece & Stahl, 2015). We might conjecture that, in many other cases, the three deficiencies are linked to simple (real or perceived) resource limitations.

2.4 ISRM Deficiencies as Situation Awareness Problems

In this paper, we consider the information security risk environment to be an "operational environment" in which information security specialists serve as "operators". A suitable theory for examining problems relating to operational situation awareness is Endsley's (1988) situation awareness (SA) theory. Although

other theoretical models of situation awareness exist, Endsley's model is considered prototypical (Rousseau, Tremblay, & Breton, 2004, p. 7), has the most research behind it, and remains the model most often applied to SA-oriented research in the present day. Endsley formally defines situation awareness as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" (Endsley, 1985, 36). As the deficiencies identified in literature describe ways in which the practice of ISRM does not perceive, comprehend, and extrapolate from elements of the information security risk environment, one can argue that these deficiencies constitute SA problems in ISRM.

3 Situation Awareness Theory

In this theory-building paper, we build on Endsley's (1988) situation awareness theory to propose an artifact that might redress the aforementioned deficiencies in the practice of ISRM. Endsley defines SA as follows:

> *SA is being aware of what is happening around you and understanding what that information means to you now and in the future. This awareness is usually defined in terms of what information is important for a particular job or goal. The concept of SA is usually applied to operational situations, where people must have SA for a specific reason, for example, in order to drive a car, treat a patient, or separate traffic as an air traffic controller.* (Endsley & Jones, 2011, p. 13)

SA occurs in three levels that one can liken to maturity stages. In level 1 SA, one perceives, or becomes aware of, "the status, attributes, and dynamics of relevant elements in the environment" (Endsley, 1995). For perception to occur, objects need to enter the real of one's awareness In level 2 SA, one compares perceptions of a situation against one's internally held understanding of, or associations regarding, this incoming information ("prototypical situations in memory;" Endsley, 1995). Level 2 SA results in comprehending, or recognizing, what the sensed data means. To comprehend incoming data, one must have adequate data in one's memory to compare it to, and the comparison process must go well. Level 3 SA occurs when one can extrapolate the implications of things perceived in the environment—to predict what will happen "at least in the very near term"—based on one's understanding of cause and effect relationships between a situation's elements (Endsley, 1995). Level 3 SA is basically akin to having a high level of comprehension because it requires pattern recognition good enough to understand what the current situation will likely develop into.

SA can occur through empirical sensory experience (i.e., "direct" perception of situational elements via the sense bases), or it can be facilitated by intermediating technologies (i.e., sensor inputs processed into computer outputs) or people's reporting. Systems are often designed to support SA by presenting people with the information that they need to perceive, comprehend, and make projections about the state of a situation. Figure 1 (next page) shows Endsley's (1995) theoretical model of SA.

4 Research Approach

We used a design science approach to answer our research question. Design science research creates *artifacts*, which can be "constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices), or instantiations (implemented and prototype systems)" that solve identified problems (Hevner et al., 2004, p. 77). While Hevner et al. presented their definition for artifact in the narrower context of information technology (IT), Peffers et al. (2007) subsequently adopted it for use in the broader context of the information systems (IS) discipline (i.e., to include organizational issues surrounding information use). Here, we argue that, "Conceptually, a design research artefact can be any designed object in which a research contribution is embedded in the design" (Peffers et al., 2007, p. 13).

Though they credit Walls, Widmeyer, and Sawy (1992), March and Smith (1995), and Hevner, March, Park, and Ram (2004) for "successfully making the case for the validity and value of design science (DS) as an IS research paradigm" (Peffers et al., 2007, p. 2) and Nunamaker, Chen, and Purdin (1990) for "actually integrating design as a major component of research" (Peffers et al., 2007, p. 2), Peffers et al. (2007) found that previous IS literature had never "explicitly focused on the development of a methodology for carrying out (design science) research and presenting it" (p. 3). Addressing this gap, they formulated the design science research methodology (DSRM) to guide design science research projects falling in the information systems discipline (Peffers et al., 2007). We adopted the DSRM and its corresponding process model (see Figure 2) for our current research project.

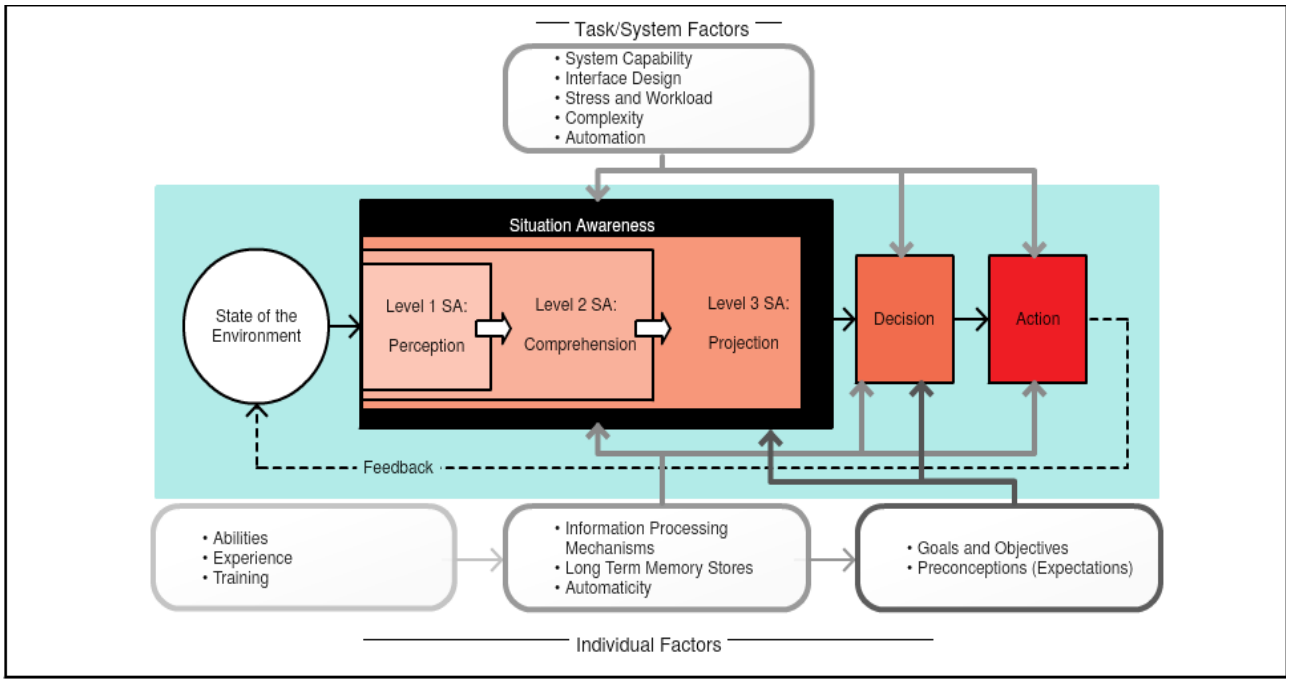

Figure 1. Theoretical Model of SA (Adapted from Endsley, 1995)

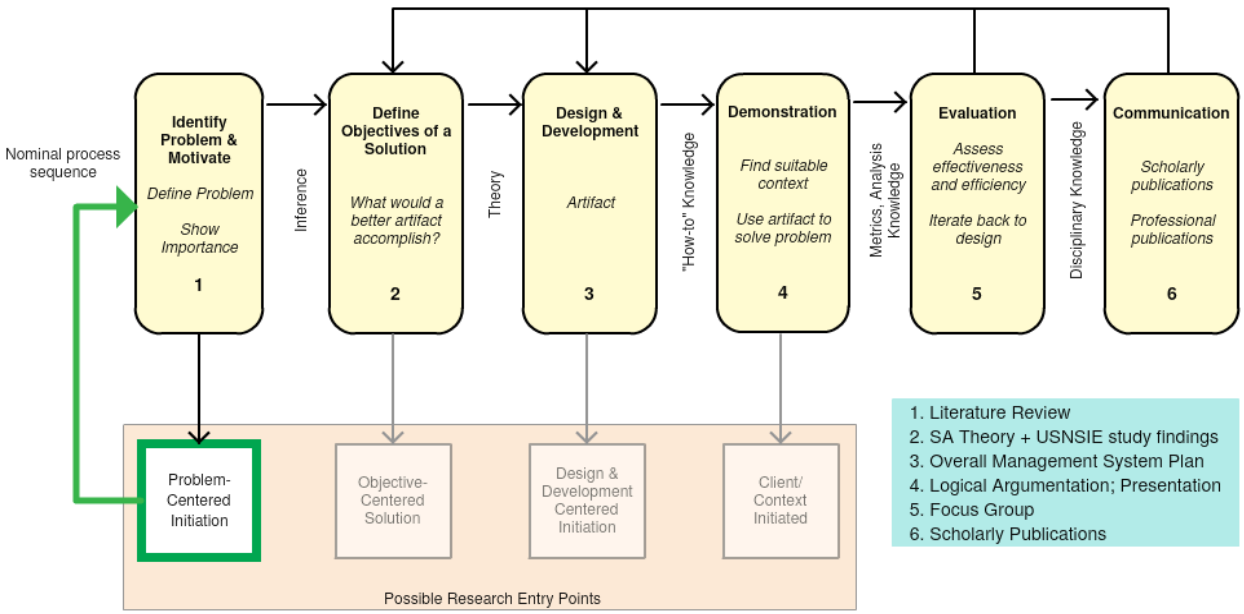

Figure 2. The DSRM Model (Adapted from Peffers et al. 2007)

As Figure 2 illustrates, the DSRM comprises six sequential activities. Peffers et al. (2007) refer to this sequence of activities as a "nominal process sequence" (the authors qualify, however, that one does not necessarily need to execute these activities in the presented numerical order).

The possible entry points for research in IS artifact design are problem-centered initiation, objective-centered solution, design and development-centered initiation, and client/context initiated. When one discovers a new problem, the entry point for research is problem-centered initiation; if a previously identified problem still exists, the entry point for research would be objective-centered solution, and so on. The entry point for research after problem-centered initiation is effectively determined by what level of

progress others in the world have already made toward developing an artifact that solves a known problem.

During the first activity (i.e., identify problem and motivate), the researcher identifies a problem and argues for its importance to motivate support for finding a solution. The researcher must then make logical inferences about what a solution to this problem might involve during the second activity (i.e., define objectives of a solution). In the third activity (i.e., design and development), the researcher, guided by theory pertinent to the problem, formally creates the artifact that fulfils the criteria of a solution.

During the fourth activity (i.e., demonstration), the researcher must correctly apply knowledge of how the artifact should work in the organization to correctly demonstrate the artifact's utility. Demonstration could involve its use in experimentation, simulation, case study, proof, or other appropriate activity. The fifth activity (i.e., evaluation) involves assessing this utility by using any appropriate empirical evidence or logical proof. The researcher can evaluate the utility by using metrics, performing analyses, or drawing on subject matter knowledge. Lastly, during the sixth activity (i.e., communication), the researcher presents the refined and validated artifact in accordance with knowledge of the disciplinary culture.

4.1 The Identified Problem that Motivated Artifact Design

The entry point for our own design science research project is "problem centered initiation". Again, the problem we identified during our review of ISRM-related literature was that many organizations have limited awareness in regard to what actually occurs in their information security risk environments, and that one can link this problem back to problems with the way organizations assess and manage information security risks. Specifically, we found three different types of problematic practical tendencies to result in limited awareness: 1) information security risk identification is commonly perfunctory; 2) information security risks are commonly estimated with little reference to the organization's actual situation; and 3) information security risk assessment is commonly performed on an intermittent, non-historical basis. As assessing the reality of a changing situation requires collecting relevant, time-sensitive information about that situation, these three tendencies result in deficient SA where present.

4.2 Defining the Objectives of a Solution

None of these three practical shortcomings describes a point of failure in some universally accepted ISRM process design. Rather, each is essentially a behavioral tendency that researchers have seen manifest itself across multiple organizations for whatever reasons. We do not know the precise array of causes and conditions that give rise to each of these problematic tendencies, but one does not need to know them to redress each tendency. Rather, one can design a process that neutralizes each tendency by creating tendency in the opposite direction. The general problem we identified is deficient awareness in regard to the information security risk environment: a lack of attention to what is actually going on, which results in misunderstandings and unrealistic assessments of risk. This general problem is the effect of the kinds of problematic behaviors that cause it (e.g., the three tendencies listed above). One can prevent (or at least significantly mitigate) the overall effect by controlling against its causes to the greatest extent possible. One can reduce or eliminate these causes via corrective/remedial action—by replacing bad behaviors with good ones, which can do achieve through designing a universal ISRM process that guides organizations away from undesirable behavior (i.e., non-rigorous information-seeking behavior) and toward desirable behavior (i.e., rigorous information-seeking behavior).

4.3 Initial Design, Development, and Communication

To determine how we might solve our research problem, we started by looking for an explanatory theory applicable our problem (i.e., a theory that explains what is actually involved in knowing what needs to be known about some operational environment). In searching for a theory, we found the construct known as "situation awareness" (SA), and we found the most appropriate SA theory for our purposes was also the most popular (i.e., that developed by Endsley, 1995). Unable to find any previous research done on the SA phenomenon in ISRM (from Endsley or anyone else), we could find nothing in the way of a ready-made process that we might introduce into ISRM to assure SA.

At this stage, we considered real-world cases that might serve as exemplary SA assurance processes, especially those pertaining to some kind of organizational context. We recognized that the USNSIE seemed to describe a system of SA-support in national security management and set out to identify the theoretical basis for this enterprise. We were interested in comparing such a theory against SA theory to

determine if one of the two might be more appropriate for our research problem than the other or if we might somehow combine the two might to suit our needs. However, a search of literature on the USNSIE revealed that researchers have accepted no single theory as a definitive "theory of intelligence" (Treverton et al., 2006). In the absence of a proper descriptive theoretical model of intelligence, we turned instead to the intelligence cycle, which is essentially a high-level process description (without a supporting theory) of what the U.S. intelligence community does to support the information needs of governmental decision makers vis-à-vis national security related issues.

We then considered the possibility that one might actually describe the USNSIE using Endsley's (1995) SA theory. We conducted an initial conceptual study to assess whether one could map elements of SA theory to the intelligence cycle in a way that corresponded with the structure of Endsley's theoretical model. We did so through a basic pattern matching variation of the illustrative method (Neuman, 2011, pp. 519-520). Both SA theory and the intelligence cycle describe information processing in the context of human consciousness/awareness. We found that we could, in fact, use SA theory as a theoretical lens through which to view the intelligence cycle and that we could adapt Endsley's theoretical model to describe both the intelligence cycle and how the intelligence cycle supports decision making. As such, we had both an exemplar and a valid theoretical lens through which to examine this exemplar.

The conceptual study led to an in-depth case study of the USNSIE, which drew on publicly available documents. We focused on identifying key actors and their functions in the intelligence community and key design features or characteristics/attributes that enable the USNSIE to work as it does. We intended to design an organizational management process with attributes conceptually analogous to those of the U.S. model. We analyzed data from the open source documents using open, axial, and selective coding methods as Neuman (2011, p. 115) describes to distill a list of key attributes for inclusion in our artifact design.

As a result, we created a theoretical model to guide organizational SA support and plans for a management system built on said theoretical model, both of which we communicated via publication (see Webb et al., 2014, for the original, though we offer an improved version in Section 5 of this paper).

4.4 Demonstration, Evaluation, Iteration Back to Design, Communication

We presented the theoretical model and plans for a management system to a focus group for evaluation. The focus group positively evaluated the overall plan. We report the results of this evaluation process in Section 6. The focus group also served a formative function in that our findings inspired iteration back to design: this paper presents an improved version of the model published in Webb et al. (2014).

5 The Recommended ID-ISRMS: General Specification

Figure 3 presents our high-level (or "big picture") model for an ID-ISRMS, which we created to redress problems identified during the literature review. This model incorporates findings from focus group research (see Section 6 of this paper) and builds on Webb et al. (2014). The focus group served a formative function as opposed to a summative function (Venable, Pries-Heje, & Baskerville, 2014); as such, the recommended ID-ISRMS design remains an a priori artifact until someone has instantiated and tested it in an organizational context.

The model describes a process by which an organization can maintain a high level of awareness in regard to its information security risk environment. The model depicts, in the general sense, how security process owners (SPOs) create intelligence via their collection and analysis efforts and communicate it to an information security manager.

The information security risk environment comprises both internal and external risks to the security of the organization's information assets and, by extension, to the security of the organization's strategic business interests. Risk factors include information security threats in the organization or in the world at large; vulnerabilities of the organization's own information assets; the dependencies of the organization's business processes and other goals on the confidentiality, integrity, and availability of its various information assets; the effectiveness of the organization's current control strategies; and the organization's own specific target profile (i.e., how and why a purposive threat agent might target it).

The model depicts two organizational entities involved in a situation awareness-formation process that precedes decision making and action in response to the state of an organization's information security situation. The first of these entities (depicted in the orange lower half of the diagram) is the information

security manager, whose activities the blue lower half of the model represents[3]. The information security manager is responsible for making critical decisions relating to ISRM. The second entity is the security process owner (SPO), whose activities the blue upper half of the model represents. Ideally, the organization will attach a SPO to each of the organization's business processes, though, for most organizations, this attachment might be limited to the most mission-critical business processes. The SPOs (and any departmental subordinates assigned to these SPOs by the organization) carry out collection and analysis activities to develop their own SA in regard to the security environment and to support the SA of the information security manager. At work in Figure 3 is a twelve-phase intelligence cycle that supports ISRM decision making.

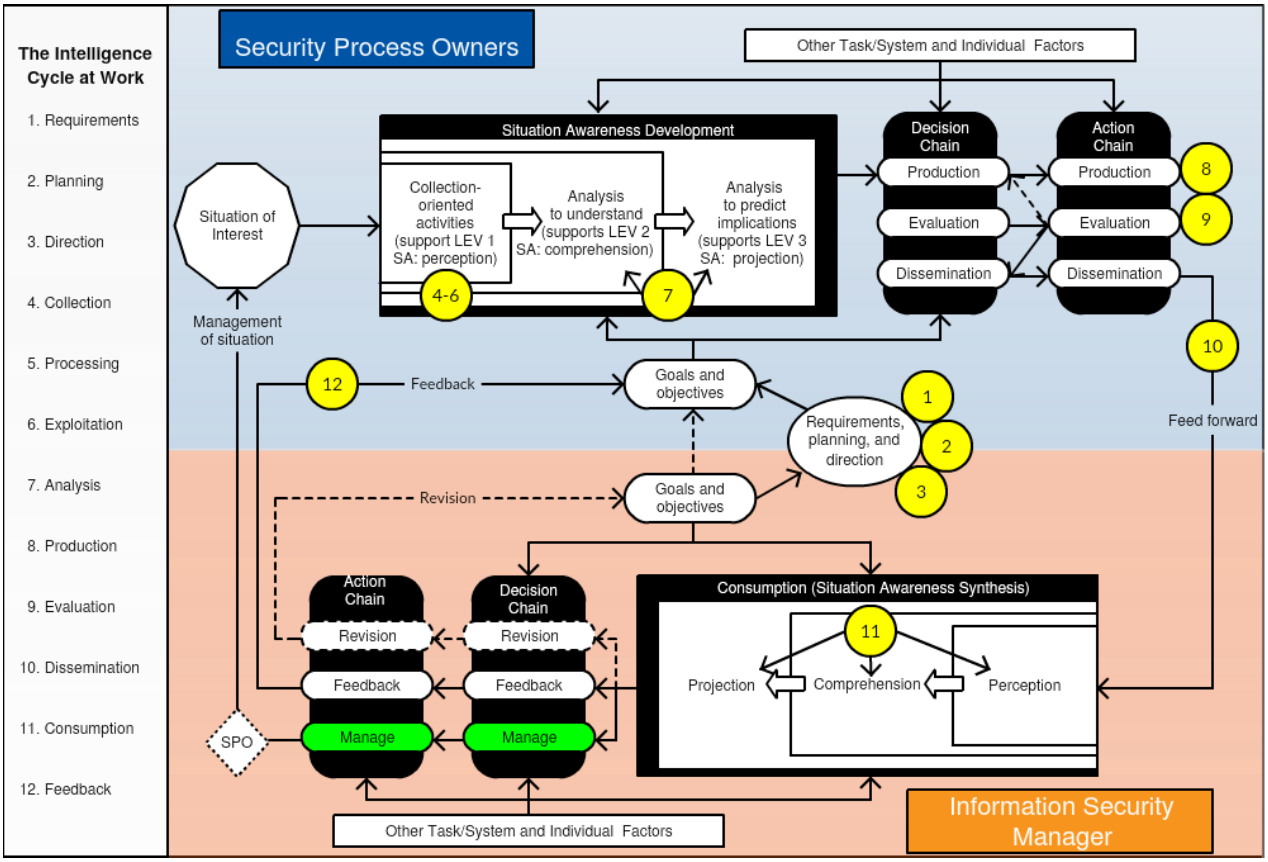

Figure 3. Organizational SA Support to ISRM

5.1 The Intelligence Cycle at Work in the ID-ISRMS Model

In phase 1, the information security manager's SA requirements for managerial decision making are articulated into intelligence requirements that the SPOs need to meet (e.g,. whether the manager has identified any breach indications, purposive or incidental threat indications, outstanding identified vulnerabilities, or positive or negative indications of control effectiveness or information asset performance in each SPO's mission area). The information security manager than carries out planning (phase 2) and direction (phase 3) to determine how team members will fulfill their specific intelligence missions (e.g., monitoring the information security risk environment of a particular business process or gathering contextual intelligence from outside sources). Next, SPOs collect (phase 4) and process (phase 5) data relating to the security statuses of information assets in their respective mission area (to include internal and external contextual factors affecting these security statuses) in order to fulfill the information security manager's issued intelligence requirements.

[3] When action is delegated to a SPO by the information security manager, the SPO effectively serves as an extension of the manager's own power.

The data collected and processed during phases 4 and 5 can include various kinds of activity logs; diagnostic readouts about the performance of hardware and software; CCTV footage; personal observations; news, industrial, governmental, or academic reports; or any other form of information that lends insight into information security risk for the organization. The collecting SPOs then facilitate "exploitation" (phase 6) by identifying and labeling indications (or possible indications) in the collected data for further analysis.

Next, each SPO formally analyzes (phase 7) the data by starting with exploitation labels and then moving into in-depth analysis to identify any additional indications that may lay hidden in the data. The SPOs then organizes their findings into an intelligence product (phase 8), which they or another team member evaluates (phase 9) to ensure that it adheres to organizational standards and fulfills the issued intelligence requirements. Once the intelligence product is evaluated positively, someone (usually the information security manager as Figure 3 depicts) disseminates (phase 10) it to the consumer.

The consumption (phase 11) of each intelligence product (during which the consumer perceives the composite elements at work in each reported situation, comprehends their meanings, and draws conclusions based on a combination of personal knowledge and product contents) leads to feedback from the consumer (phase 12) as to whether the product has fulfilled their requirements. Depending on the SPO's findings, the information security manager may revise their own SA/intelligence requirements or may order (or personally carry out) some action in response to a particular situation.

5.2 Intelligence-supported Managerial Decision Making and Action

Depending on the information security status of a particular business process, managerial decision making and action can take any of three different courses: deliberate inaction, remedial action, or the recommendation that intelligence requirements (or even organizational goals and objectives) be revised. Deliberate inaction is the logical course of action when incoming intelligence suggests that the business process is currently secure or when a particular type of risk is consciously accepted (i.e., because it is considered highly unlikely to occur or because it is expected to carry a negligible impact).

However, in the event that an SPO's findings indicate an unacceptable source of risk (e.g., a newly identified vulnerability to a particular information asset type), the information security manager needs to ensure that they (i.e., the security manager) take the appropriate remedial action. They can do so either by checking that the reporting SPO has performed the necessary action (if the manager has delegated power to the SOI or if the SPO already has authorization under policy) or by ensuring that the SPO has provided any necessary resources requiring higher authorization (from either the manager or the executive level), if available, or requested if currently unavailable. Lastly, if the SPO's analysis uncovers (or if the information security manager notices) a new or previously unidentified issue with implications for the organization's strategic interests, the manager may recommend revising policy to accommodate or address that issue. Depending on the issue, the manager might accompany the recommendation with an order for remedial action under existing policy.

5.3 A Formal ID-ISRMS Design Theory

Several authors working in the information systems domain have published papers in which they argue that one should accompany a design science artifact with a design theory that describes the artifact's functionality in a particular standardized format. Each of these papers has proposed its own format for structuring a design theory. Walls et al. (1992) proposes a formulation in which one specifies the design theory = across six different categories: meta-requirements, meta-design, kernel theories, testable hypotheses for process and product, design method, and kernel theories for process and product. The formulation that Gregor and Jones (2007) suggest essentially expands on the formulation that Walls et al. suggest; however, Gregor and Jones argue that some of the category terms that Walls et al. use should be changed and that two additional categories should also be included in the specification of a design theory (constructs and artifact mutability), which results in a total of eight categories. Baskerville and Pries-Heje (2010) criticize both of the aforementioned formulations for being overly overcomplicated and, invoking Occam's razor (i.e., that a design should be as simple as possible), propose that the format for a design theory should be limited to two main descriptive categories: the general requirements that need to be met and the general components of a design intended to meet these requirements.

Venable (2013) notes that the ostensible differences between the Walls et al. (1992) and Gregor and Jones (2007) formulations are largely a matter of semantics (i.e., the authors use different terminology to

refer to the same ideas) and agrees with Baskerville and Pries-Heje's (2010) assessment that a better design theory format would be simpler than Walls et al.'s or Gregor and Jones' (2007) format. However, Venable argues that Baskerville and Pries-Heje's format is *too* simple (in that it does not explain how and why a design solves a problem). As such, he proposes a fourth formulation that offers more specification categories by reincorporating several categories that Walls et al. and Gregor and Jones recommend. The crux of Venable's argument is that a design theory should clearly present an artifact's utility and how that utility leads to the artifact's intended purpose. Venable offers a diagram ("proposed simplified design theory formulation") to guide theory design, but one can argue that this particular representation is itself misleadingly oversimplified in that one cannot really link its "general design" content to its "general requirements" content in the kinds of straightforward utility statements about efficacy, effectiveness, or efficiency, that the diagram implies are possible.

Any of the aforementioned formulations for a design theory specification is arguably preferable to the other because selecting one over another depends on one's perceived priorities (i.e., what things someone believes to be more important to communicate when discussing artifact design). In this paper, we use Gregor and Jones' (2007) format for its more comprehensive treatment in hopes that it best represents information of potential interest to the reader. Table 2 presents a design theory specification that follows Gregor and Jones' format.

Table 1. The Recommended ID-ISRMS Design Theory (Adapted from Gregor & Jones, 2007, p. 322)

Design theory component	Description specified by Gregor and Jones (2007)	ID-ISRMS component
Purpose and scope	*"What the system is for": the set of meta-requirements or goals that specifies the type of artifact to which the theory applies and in conjunction also defines the scope, or boundaries, of the theory*	The recommended ID-ISRMS is an organizational management system designed to support SA and redress common practical flaws identified in literature: 1. Perfunctory risk identification 2. Unsupported risk estimation 3. Intermittent and ahistorical risk assessment This ID-ISRMS guides organizational behavior using an intra-organizational intelligence cycle framework that can also loop inputs and outputs inter-organizationally.
Constructs	*Representations of the entities of interest in the theory.*	**SPO-level entities**: 1. Situation of interest: subset of organizational information security risk environment (mission area) 2. Security goals and objectives 3. Task/system and individual factors 4. Requirements, planning and direction 5. Collection activities (data collection→processing→exploitation) 6. Analysis activities (comprehension→prediction) 7. Decision chain activities (production→evaluation→dissemination) 8. Action chain activities (production→evaluation→dissemination/feed forward to manager) **Manager-level entities**: 1. Situation of interest: overall organizational information security risk environment 2. Security goals and objectives 3. Task/system and individual factors 4. Requirements, planning and direction 5. Consumption activity 6. Decision chain activities • Revision of goals and objectives • Feedback to SPO • Manage situation 7. Action chain activities • Revision of goals and objectives • Feedback to SPO • Manage situation Management delegation option

Table 1. The Recommended ID-ISRMS Design Theory (Adapted from Gregor & Jones, 2007, p. 322)

Principles of form and function	*The abstract "blueprint" or architecture that describes an IS artifact, either product or method/intervention.*	The process model (see Figure 3) serves as the recommended ID-ISRMS blueprint. The SPO develops SA by collecting, processing, exploiting, and analyzing intelligence. In producing, evaluating, and disseminating intelligence products, the SPO supports the manager in synthesizing SA. The SPO designs products to enable managers to perceive, comprehend, and project to element states in the information security risk environment.
Artifact mutability	*The changes in state of the artifact anticipated in the theory, that is, what degree of artifact change is encompassed by the theory.*	The model offered in Figure 3 is a high-level, generic process description. At this level, mutability of the artifact would chiefly pertain to changes in incorporated roles; that is, the possibility of one or more entities apart from the proposed SPO construct executing intelligence activities; or the possibility of a decision maker apart from an information security manager making decisions that affect the risk environment. An organization's context and business objectives would shape the details in this process (i.e., the specific attributes of a particular real-world ID-ISRMS instantiation).
Testable propositions	*Truth statements about the design theory.*	Primary proposition: one can improve SA in ISRM by implementing the recommended ID-ISRMS design. • Proposition A: the recommended ID-ISRMS design will redress flaw 1 (see purpose and scope row above for the three flaws) by making information security risk identification more rigorous. • Proposition B: the recommended ID-ISRMS design will redress flaw 2 by increasing the evidentiary basis for information security risk estimates. Proposition C: the recommended ID-ISRMS design will redress flaw 3 by introducing a continuous assessment process with archived documentary outputs.
Justificatory knowledge	*The underlying knowledge or theory from the natural or social or design sciences that gives a basis and explanation for the design (kernel theories).*	The justificatory knowledge guiding process design combines a kernel theory borrowed from the human factors research domain (SA theory) and findings from a case study of the U.S. intelligence community. SA theory holds that human awareness about a particular situation must be built in progressive stages of cognitive information processing: perception, comprehension, and projection. Findings from the case study strongly suggest that the intelligence cycle functions as a form of organizational information processing in support of this cognitive process. Thus, in an organizational context, one can expect an intelligence cycle to support a human decision maker's SA.
Principles of implementation	*A description of processes for implementing the theory (either product or method) in specific contexts.*	One can adapt the process in Figure 3 to any organizational context. Large organizations might create multiple SPO roles, and small organizations might create one or two SPO roles. In very small organizations with very limited resources, the information security manager might actually perform the SPO functions; in such a case, one would likely want to revert to Endsley's original operator-level model.
Expository instantiation	*A physical implementation of the artifact that can assist in representing the theory both as an expository device and for purposes of testing.*	Ultimately, someone needs to implement and test the artifact in a real organization (e.g., via action research). As no one has yet done so, the proposed ID-ISRMS remains an a priori artifact.

6 Focus Group Findings

We conducted a focus group with six experienced information security specialists, five of whom actively participated in the discussion around the proposed management plan. For their anonymity, we refer to the participants in this paper as P1 through P6. They included the senior information security specialist at a leading consulting firm in the computer and network security industry (P1). the chief information officer at an Australian Federal Government organization (P2), a senior information security analyst from a major ICT consulting firm in Australia (P3), an information security specialist with a background in national intelligence (P4), the lead security specialist at a major bank in Australia (P5), and the security risk and

compliance manager / information security architect at a multinational telecommunications company (also a former consultant; P6). The participants had approximately 70 years' combined experience in the information security field. As consultants, three of the participants had experience working with numerous organizations apart from their principal employers.

We presented the focus group participants with a management system plan that had two major attributes:

- The distribution of ISRM responsibilities across specialists (security process owners) who are attached to business processes.
- The continuous execution of an intelligence cycle in which SPOs manage the collection and analysis of information security risk intelligence to support managerial SA for informed decision making.

The focus group participants indicated that they believed the three deficiencies identified during the literature review were actual and current problems, and that they believed that the proposed artifact would redress these problems by significantly improving SA in ISRM. All of the focus group participants indicated that the high-level model presented to them described a viable SA-support process that they could apply in ISRM. Figure 3 shows this high-level model, which we have since redesigned to more clearly distinguish between different process stages.

Due to time restrictions and the danger of overloading the focus group participants with too many details, we limited the focus group discussion to the above high-level management system plan.

6.1 Focus Group Commentary on the Anticipated Usefulness of the Recommended ID-ISRMS

In the sections that follow, we comment on the utility of the ID-ISRMS given the systemic deficiencies in the practice of ISRM.

6.1.1 ID-ISRSMS Potential Benefits for Information Security Management

By the end of the focus group discussion, P1, P2, P3, P5 and P6 all agreed that the recommended ID-ISRMS would probably enable organizations to monitor risk on a continuous basis (P4 did not express an explicit opinion on this point). P1 commented that one could probably expect the recommended ID-ISRMS to ease the management of information security issues: "I think if you get a security person embedded with each critical application… that'll drive culture change. I think that'll actually improve security right there…". After offering several examples of how this might be the case, P1 commented that one could expect embedding SPOs into business processes to facilitate better managerial control. P5 commented that the intelligence outputs of the recommended ID-ISRMS could offer good support to managerial decision making: "I think that if it's a processed piece of intelligence that is given to them, then it should, theoretically, make the risk manager's job easier because it's all laid out for them…what the issue is.". P2, P3, P5 and P6 all commented that the recommended ID-ISRMS would probably help managers identify and attend to information security issues that might otherwise go unnoticed.

6.1.2 ID-ISRMs Potential Benefits for Richer Insight into Organizations' Information Security Risk Environments

P1, P2, P3, P5, and P6 all felt that using the recommended ID-ISRMS could enhance SA in regard to organizational information security (P4 did not express an opinion on this point). When asked whether one might expect the recommended ID-ISRMS to yield quality evidence regarding the status of the implementing organization's information security risk environment, P2, P3, P5, and P6 all answered in the affirmative. P1 commented that, "in a situation where…you embed a security expert in each team: absolutely, you will get better input—intelligence". P6 commented that one could probably expect the recommended ID-ISRMS to yield "better information" than other approaches to information security management and that "the richer the information, the better evidence you'll have". P5 agreed that the recommended ID-ISRMS would probably yield "better" and "more up-to-date" information and argued that providing such information "allows a better decision". P2 also felt that the process could only help: "This kind of process would be useful to increase visibility over what's going on: to catch it…. Anything other than, 'oh, what do you think?'…. 'Oh well, maybe it should be a 4, or maybe it could be a 3' would be useful.". P3 saw particular value in the fact that the recommended ID-ISRMS "opens up a new sense of risk that IT people are not usually open to" and "helps you to increase the richness of your risk register—

or your risk *process* (emphasis in original)". Both P2 and P5 expressed keen interest in the combined internal/external focus of the recommended ID-ISRMS's intelligence and analysis activities. On the collection of intelligence in organizations, P5 said:

> *If someone's…embedded in the team and the guy is sitting there, going, "this guy's not doing the right thing", then it doesn't matter if it's on a physical piece of kit or a cloud piece of kit, or his PC or whatever, at least that intelligence is getting back to the risk manager and (s/he's) making informed decisions about what is happening in the organization.*

On the exploitation of intelligence from external sources, P5 said:

> *If you've got the external sources coming in…and you're someone who's sitting there going, "OK, we've got this product: these are the things that we need to start looking at"…. I think that there is a benefit of them driving that to the risk manager and saying, you know…, "this intelligence shows that these are vulnerable to this and we need to start doing this, or this"…. There is benefit in that.*

On the collection of intelligence in the organization, P5 said:

> *The thing I like about the theory of deploying something like this is that it's not just that kind of intelligence you'd get from, I don't know, some vendor that makes a product. This is going to be intelligence outside the IT box…how people are behaving; what exceptions there are to the processes that people are actually doing on the ground; what we believe them to be doing. You're going to get much better visibility: three-dimensional visibility, as opposed to "oh, Shellshock's there" or "Heartbleed's there" or "that system needs a patch". It's not just about system vulnerabilities. To me, that's…how I see it as being useful.*

After we explained that the externally oriented intelligence collection would draw on industry sources and open source intelligence from academia and government, P2 noted that it would be good if the Australian Government also provided non-technical forms of information security-pertinent intelligence to organizations: "The Australian Signals Directorate…produce and circulate an information security manual, which is a publicly available document with a list of technology controls…. It would be useful to have something additional to that.".

6.1.3 ID-ISRMs Potential Benefits for Faster Response to Information Security Issues

Five of the six participants (P1, P2, P3, P5, and P6) could imagine situations in which having the recommended ID-ISRMS in place would probably lead to quicker issue resolution (P4 did not express an opinion on this point). P1 and P5 agreed that, in most organizations, the responsibility for identifying and reacting to information security issues generally falls on information security managers and that this arrangement results in reduced awareness and slower response times than would be the case if SPOs were embedded in the organizations' business processes. P1 said:

> *If you've got a security expert next to you, you'll just ask them a question, right? As opposed to "oh, I've got to go to information security or go through a process, and then I've got to get a security engineer to put it to them, and I've got to put them on my project code", and—you know?—you've got like a one month process before you can ask the question, right? If they're in your team, you go, "what should our password length be?". Right, and they'll go, "well 12 characters" or set a complexity, or whatever, and they should be able to answer it. So I can see having a security resource in each team being really effective in increasing controls.*

P6 offered Shellshock and Heartbleed as examples of information security issues that one might resolve faster via the recommended ID-ISRMS: "having a process like this (points at the diagram)…would get [you] a faster answer".

6.1.4 ID-ISRMs Potential Benefits for Helping Organizations to Deconflict/Coordinate their Information Security and Business Strategies

Though no participant argued against the idea of integrating information security and business strategies, P1, P2, P3, P5, and P6 all seemed to be pessimistic about this becoming a reality in most organizations (P4 did not express an opinion on this point). Nevertheless, all five could imagine—at least in theory—that the recommended ID-ISRMS would support this aim.

P6 noted that one can often identify or interpret risk somewhat myopically; that is, relative only to what the person who is assessing the risk is trying to do: "that the risk owner can say "that's *this* value to *us*. They can't see risk outside of that side of it" (emphasis in original)—a statement with which P1 agreed. P2 and P3 both commented that one could probably not expect most organizations to fully appreciate the strategic significance of information security. P6 saw the value in equating information security with information *process* security because doing so ties information security back to the functionality of the business: "How does the business do these things? …it's only after that that you start to draw out…. This is where the security aspects are, you know?". P6 felt that the recommended ID-ISRMS goes so far in the direction of reconnecting information security to business functionality that one might better market it as a "business process optimization" framework. P1 also anticipated that the SPO role in particular could be valuable toward bridging business and information security:

> *That's the point of someone being part of the business in which they understand the applications, the outcomes and the business objectives…. If they wear two hats…, they won't be, "thou shall apply the rules" and "thou shall do security because security's the most important thing in the universe".*

Giving the example of an obstructive information security policy, P5 saw the value in having individuals who can advocate for business processes monitor information security from within those processes:

> *This isn't working because the policy's too strict; the guys are going to go through twenty different jump boxes to get to that…or do twenty different things to do that outcome…you know? I think there's value there…. I think that intelligence is driven out from that is a good thing.*

6.1.5 Types of Organizations that Might Benefit From Implementing ID-ISRMS

P1, P2, P3, P5, and P6 had varied opinions about which kinds of organizations might benefit most from the recommended ID-ISRMS (P4 did not express an opinion on this point). On the topic of what types of organizations might benefit most from the recommended ID-ISRMS, P6 remarked, "Well, I think all organizations would benefit….economically, if you've got processes that you can standardize…or you can get aspects standardized of…, then you'll get a lot of benefit out of it.". Both P3 and P5 made comments suggesting that the recommended ID-ISRMS could be appropriate for any organization. P2, who worked in a small to medium-sized Australian federal government organization, commented that the recommended ID-ISRMS would probably have value for P2's organization, whereas P1 opined that larger, higher maturity information security organizations such as banks would probably benefit most from using the recommended ID-ISRMS.

6.1.6 How ID-ISRMS Could Be Used as the Basis for an Intelligence Sharing System between Organizations or Between Organizations and Government

When we suggested that one might also use the recommended ID-ISRMS to feed intelligence forward to organizations such as the ASD or ASIO, P1, P2, and P5 all responded enthusiastically to this prospect (P3, P4, and P6 had no comments on this point). In P1's words, "Something like that'd be awesome. Something like that would actually create better intelligence.". P2 was particularly interested in the possibility of receiving threat intelligence from similar organizations:

> *I was interested in the external intelligence feeding in….because looking at this process from a smaller organization point of view, it would be useful to go and get external information—from like organizations [that] may face similar threats*.

6.2 Focus Group Participants' Caveats and Concerns

In this section, we present findings from the participants that relate to potential hindrances in implementing or effectively executing the recommended ID-ISRMS process in organizations.

6.2.1 Potentially Confounding Political and Cultural Factors

All of the participants believed that people who worked in an organization that implemented the recommended ID-ISRMS could easily undermine it. P1 and P6 both warned that one could expect political factors such as personal agendas to skew risk assessments if allowed to do so. P1, P5, and P6 made comments that suggested that one would need to somehow safeguard the objectivity of intelligence and decision making outputs from the recommended ID-ISRMS against intentional manipulation. P1 remarked

that “[people] will generally be incentivized one way or another to either raise or lower the risk…. If they want funding, they’ll raise the risk; if they want their bonus, they’ll lower the risk.”.

P1 went on to warn that, “when you do a model like this, you need to either make sure that the people who can influence it aren’t incentivized to either corrupt the rating or that the people who rate it are truly independent”. P5 commented that people often accentuate risk in order to secure a budget. P6 remarked that people can sometimes be “captured” and essentially pressured into saying or doing things to suit others’ agendas. P4 warned that an informal reporting structure could result in corrupted intelligence if products were permitted to be vague or if their contents were communicated insecurely or otherwise in less reliable ways (e.g., verbally from person to person).

Several participants commented on the importance of formal authorization/mandate. P2 considered that other employees might regard the SPO as an interloper: “Imagine that it’s the finance area; how are they going to react to having a security person embedded in there?”. Likewise, P1 said that, unless the SPO has the explicit mandate to collect all of the necessary forms of intelligence, others would likely view the SPO as an annoyance or to otherwise treat him or her dismissively: “My experience [is that]…they’ll be tolerated up until a point—until there’s a deadline—and then they’ll be told to ‘shut up’”. P4 also anticipated that staff members could view the SPO as a kind of “obstacle” to clear. P3 recommended that probably the best way to preclude these kinds of problems would be to adopt a reporting structure in which SPOs report to someone who outranks the personnel with whom the SPO is embedded.

6.2.2 Resistance is Possible (if not Likely)

All of the participants felt that the proposed ID-ISRMS constituted an unfamiliar approach that many people might not be comfortable with. P3 stated that, in P3’s experience, the information security manager did not practice risk management: “the business unit is responsible for risk management; the information security manager only guides or facilitates the process”. P1 suggested that the recommended ID-ISRMS represented an overly rigorous approach to information security that most organizations would not see the value in (“I don’t think you’ll get it across the line because I don’t think any organizations will see the cost-benefit analysis of it”). P1 felt that the exceptions to this rule might be organizations that already had mature information security regimes that they were interested in making even better: “You’re on top of your game and then you’re going to embed these people to give you knowledge above and beyond that? I can see that working for you…your ‘life-and-death’ and your billion-dollar systems, right? I can see that working.”.

Several participants mentioned resentment about someone monitoring their behavior. P4 saw the proposition as a sign of deteriorating values in organizations: “It kind of begs the question, ‘where is the room for trust in an organization?’. It’s almost like there’s no room for trust. Things like their culture and policy have no integrity in them.”. P6 suggested that someone tasked with monitoring employee behavior would be “an expensive resource that’s sitting around, looking for a needle in a haystack” and went on to label such an employee a “saboteur”. P2 and P1 also both made sarcastic comments about someone in such a role; they used the terms “spy” and “commie NARC”, respectively, and P3 commented that “instead of this security person embedded, you need a spy…trained by the KGB”.

P6 suggested that, while it may be a good idea to do so, most organizations aren’t used to looking at business processes and information security processes as interdependent functions and anticipated that one could expect many people to have difficulty doing so (“they don’t think outside their box”). Both P2 and P3 anticipated that the design of the recommended ID-ISRMS could be contentious for many organizations because they might not see the value in it. P3 commented that an organization that “ticks the box for compliance reasons” would be unlikely to see the value of the SPO role.

Both P5 and P6 anticipated that convincing organizations of the ID-ISRM’s utility may be difficult because it would require training and embedding personnel for the SPO role (P6: “You’ve got to convince the management in there that it’s worthwhile”; P5: “Return on investment…; it’s a big thing”). P5 went on to conjecture that organizations that have not already adopted a risk-based approach to information security would probably be non-receptive to the ID-ISRM given its risk-management orientation. P1 and P6 both shared an initial impression that the recommended ID-ISRMS would probably be labor intensive or otherwise expensive to implement and run. P6 commented that the ID-ISRMS model we presented seemed to represent “an extremely heavy framework”.

6.2.3 Obtaining the SPO Skill Set

P1, P2, and P6 all felt that it could be difficult to find or train up people for the SPO role (P3, P4, and P5 did not have any comments on this point). Ideally, SPOs would have knowledge of information security, risk management, and the functional intricacies of their assigned business process (which have been mapped in terms of their information infrastructure). As P1 noted, establishing this knowledge would most likely require consultation and coordination: "if you give it…straight to a risk—security—person, they're not going to understand the system. If you give it straight to the asset owner, they're not going to understand risk—or, intelligence—and what they should actually be collecting". Both P1 and P6 suggested that they did not expect many people to have the skills required to act as an SPO. P1 thought that "good security people" are in short supply and that having multiple personnel with the requisite SPO skill set distributed throughout an organization would be prohibitively expensive in most cases. Similarly, P6 commented that developing a holistic and comprehensive understanding of risk in the context of any particular system requires a level of skill that few people actually have.

P1 warned that attempting to solve this issue by putting less-skilled personnel into the SPO roles would probably itself result in lower quality intelligence and, by extension, deficient managerial situation awareness. P2, giving the example of a finance related business process, noted that it may be difficult for an information security specialist to develop a comprehensive understanding of such a process and suggested that it may make more sense to train the business process owner up in information security: "they're going to know the business process much better, and they're going to know about the exceptions to the business process". Similarly, P1 stated that, from personal experience, "it's easier to teach a person a basic security process than it is to teach another person an understanding of a business unit, culture, or process". P6 commented that either way could work (i.e., training an information security specialist in the business process or training a business process owner up in information security) depending on the person's operational competence and social skills. In addition to having the requisite subject area knowledge, P6 stressed that the interactive nature of the SPO role also meant that whoever served in this role would need to be a "people person".

6.2.4 ID-ISRMS Success Hinges on How Standardizable it is Across Organizations

P1, P5, and P6 all argued that the recommended ID-ISRMS design would need to be as user friendly as possible (P2, P3, and P4 did not comment on this subject). P6 felt that the success of the recommended ID-ISRMS would largely hinge on the extent to which one could standardize its component activities ("Economically, if you've got processes that you can standardized…or you can get aspects standardized of, then you'll get a lot of benefit out of it"). P6 also commented that the recommended ID-ISRMS might otherwise represent an overly "heavy framework" for most organizations to implement:

> *You've got to develop the frameworks, you've got to develop the standards…. You've got to do a whole heap of work…. The actual person who gets embedded is—the SPO—is the cheap part of this. It's the time taken to get them up to speed; the time taken to embed this in the organization.*

P1 noted that standardizing intelligence collection across organizations could be difficult, however, because "internally, they're pretty diverse" and warned that "if you're trying to put a cookie-cutter kind of checklist of the status of systems on it, you're going to come out with rubbish data. Either they're going to rate it wrong or not rate it or…the description's not going to be appropriate for that.". P5 agreed with these statements and added that practitioners probably could not be expected to deduce what to do in the absence of instructions tailored to their particular situations.

7 Discussion

Ultimately, the focus group data validated the artifact. Five of the six focus group participants stated that they believed the recommended ID-ISRMS could, if properly executed, redress the three problematic tendencies we identified during the literature review. However, organizations' resource limitations would necessarily determine how organizations actually implemented the recommended ID-ISRMS. For example, small to medium-sized organizations may only be able to attach one SPO to a particularly critical business process, to assign multiple business processes to a single SPO, or even to assign all collection and analysis duties to a single person (e.g., the information security manager). Conversely, large, highly competitive, or otherwise high-stakes organizations (e.g., in the defense, credit, banking, or pharmaceutical industries) may need to employ numerous SPOs across all of the organization's business

processes. Regardless of the number of personnel involved, the participants noted that one could reasonable expect the recommended ID-ISRMS to improve ISRM through its proactive support of managerial SA and its emphasis on evidence-based decision making. We discuss these strengths further in Section 7.1.

7.1 How the Recommended ID-ISRMS can Address the Common Deficiencies Identified in Literature

We purposefully designed the ID-ISRMS model we present in this paper to facilitate thorough, investigative, and continuous risk assessments that maximize SA in ISRM. We focused on providing organizations with an approach that guides practice away from the perfunctory, speculative, and intermittent approaches criticized in literature.

Organizations could use the recommended ID-ISRMS to link information security directly to their strategic business interests. Attaching SPOs to an organization's business processes agrees with recommendations from Coles and Moulton (2003) and Fenz et al. (2009) that one should perform ISRM with an eye on business processes. By requiring the detailed mapping of business processes in terms of their complete "information infrastructure" and by requiring SPOs to actively track the effectiveness of control strategies currently in use, the proposed ID-ISRMS can potentially redress the problems of fragmentary information asset inventories and murky asset ownership that Al-Ahmad and Mohammad (2012) cite and can reduce confusion in regard to an organization's current defense posture or countermeasure options (as Fenz et al. (2014) note).

Because it pushes for one to support ISRM decisions with real evidence and quality analyses that consider business and information-security needs, the recommended ID-ISRMS could help to minimize the possibility of inappropriate control strategy decisions, which include those based on unrealistic perceptions of risk such as those that Rhee, Ryu and Kim (2012) and Qian, Fang and Gonzalez (2012) report and control selections that can end up hindering operations (as Ahmad, Bosua, and Scheepers (2014) note) and creating new problems when employees try to work around them (as Pfleeger and Caputo (2012) note).

The recommended ID-ISRMS delegates responsibilities to the members of a permanent and perpetually operational ISRM team, which agrees with Young and Windsor's (2010) warning that one needs to distribute authorities throughout an information security enterprise for it to function well. This distribution mitigates data overload problems such as those cited under the first and second deficiencies. Collecting and analyzing intelligence across an organization, from the information asset level up to the business-process level, could enable multidimensional strategic analyses beyond the "entire computing infrastructure" analyses that Nazareth and Choi (2015) recommend. However, because a central authority controls the recommended ID-ISRMS (with direct reporting between the information security manager and the executive level), it might also preclude the kinds rogue decision making that Al-Ahmad and Mohammad (2012) note.

The recommended ID-ISRMS assumes a proactive posture that stands in stark contrast to the "reactive management approach" that Qian et al. (2012) criticize. Because the recommended ID-ISRMS focuses on rigorously investigating organizations' information security risk environment, it could direct practitioners away from the kinds of superficial but technically standards-compliant approaches to information security that Von Grebmer (2006, p. 40), Siponen (2006), Matwyshyn (2009), Shedden et al. (2010), Al-Ahmad and Mohammad (2012), and Flores et al. (2014) note. Rather, it actively collects the kinds of empirical evidence that numerous authors (e.g., Baker et al., 2007; Fenz et al., 2014; Vroom & Von Solms, 2004; Da Veiga & Eloff, 2010; Qian et al., 2012; Crossler et al., 2013; Da Veiga & Martins, 2015; Baracaldo & Joshi, 2013; Crossler et al,. 2013; Ab Rahman et al., 2015; Friedberg et al., 2015) have found organizations commonly ignore. Through relying on intelligence over guesswork, the recommended ID-ISRMS might address many of the broad but also fundamental problems with ISRM that Baskerville (1991), Parker (2007), and Utin, Utin & Utin (2008) have drawn attention to.

With its attention to all information asset types supporting each business process, the recommended ID-ISRMS breaks away from the outmoded IT-centric paradigm that Jaatun et al. (2009; "information security as a technical issue") and Reece and Stahl (2015; the "technical checklist approach") refer to. One might expect this genuinely holistic approach to information security to reduce or eliminate many of the risk-identification failures reported in literature. Examples of risk sources that one could more easily identify using the recommended ID-ISRMS approach include intangible knowledge assets (Shedden et al., 2011;

Ahmad et al., 2014), complex asset interdependencies (Parker, 2007; Utin et al., 2008; Nazareth & Choi 2015; Friedberg et al., 2015), non-technological contextual factors (Vroom & Von Solms, 2004; Al-Ahmad & Mohammad, 2012; Da Veiga & Eloff, 2010; Da Veiga & Martins, 2015; Flores et al., 2014; Parsons et al., 2014), employee behavior (Kowalski, Cappelli, & Moore, 2008; Colwill, 2009; Ruighaver, Maynard, & Warren, 2010; Lim, Ahmad, Chang, & Maynard, 2010; Stewart & Lacey, 2012; Guo, 2013; Crossler et al., 2013), historical threats and vulnerabilities (Ahmad et al., 2012; Ab Rahman et al., 2015), and strategizing threat agents (Parker, 2007; Raiu, 2012; Baracaldo & Joshi, 2013; Fenz et al., 2014; Friedberg et al., 2015).

In particular, the recommended ID-ISRMS could support SA's temporal dimension. Because the recommended ID-ISRMS executes a continuous intelligence cycle in support of ISRM, it may reduce or eliminate the kinds of problems that Hulme (2004), Rees and Allen (2008), Schmittling (2010), Crossler et al. (2013), and Da Veiga and Martins (2015) report—problems associated with intermittency (i.e., inattention *during* particular intervals of time). The continuity of the intelligence cycle could reduce SA failure at the level of perception (level 1 SA) by increasing the chance that organizations would notice a development occurring at any point in time. Furthermore, the archiving of intelligence products in the recommended ID-ISRMS could support long-range organizational learning by providing a body of standardized historical data that one could reference in future information security risk assessments, which may redress many problems relating to inattention *across* intervals of time. Long-range organizational learning could reduce SA failures at the levels of comprehension (evel 2 SA) and projection (level 3 SA) by supporting the memory required to recognize emerging patterns in incoming data.

When complemented with the routine intelligence sharing and dissemination activities incorporated into the recommended ID-ISRMS design, its record-keeping practices could help safeguard the implementing organization against the kinds of operational dissociation, stove-piping, amnesia, and communication breakdowns that Jaatun et al. (2009), Shedden et al. (2011), Ahmad et al. (2012), and Tøndel et al. (2014) have observed. Lastly, via circulating memoranda and reports that cite SPO intelligence findings, the information security manager would act as the organization's own in-house intelligence advisor, which would help to ensure that all stakeholders remain "in the loop" in regard to information security issues. This level of participation by stakeholders could reinforce the organization's information-security culture and mitigate those information security awareness and education issues that Rhee et al. (2012), Da Veiga and Martins (2015), Myyry et al. (2009), Flores et al. (2014), and Parsons et al. (2014) identify.

Because we designed the recommended ID-ISRMS to produce quality, actionable information security risk intelligence, we anticipate that it could also be highly conducive to sharing information between organizations or with government agencies. Crossler et al. (2013), Werlinger et al. (2010), Fang et al. (2011), Fenz (2012), Tamjidyamcholo & Al-Dabbagh (2012), Feledi et al. (2013), Tamjidyamcholo et al. (2013), and Tamjidyamcholo et al. (2014) have all argued that one can expect sharing knowledge about risk between information security professionals to increase managerial competency and reduce information security risks to organizations as a result. A community intelligence sharing arrangement could yield more reliable intelligence than vendor products do given that, as Parsons et al. (2014) have noted, these products can sometimes be biased in the interest of selling security solutions.

8 Conclusions and Future Work

The intelligence-driven information security risk management system (ID-ISRMS) that we propose in this paper can make a significant contribution to theory and practice by providing organizations with a management system for institutionalizing organization-wide situation awareness into their ISRM practices.

To ensure that the recommended ID-ISRMS functions as intended, however, organizations need to recognize several potentially confounding factors. First, if decision makers in the organization are vague about their own intelligence requirements, it will be virtually impossible to conduct an effective intelligence effort because no one will have a clear idea about what intelligence needs to be collected or why or about how this data should be analyzed to arrive at relevant conclusions about the state of the information security risk environment. Second, SPOs require unobstructed access to their collection targets; their efforts will be hindered wherever information owners are unwilling or unable to share information in a timely manner. Third, from a resourcing perspective, the ID-ISRMS presented here involves several specialized personnel; as such, it may only be feasible for organizations who operate in highly competitive or particularly risk-sensitive industries.

Other organizations may prefer to limit the scope of the intelligence effort to monitoring a few critical business processes and assign SPOs to these processes but not to others. In some cases, an organization's leadership may not consider a business process strategically important enough to warrant constant monitoring (it may be neither possible nor desirable, for example, to assign a SPO to a business process that has been effectively outsourced to another organization). Some smaller organizations with fewer resources might even limit one SPO's responsibilities to a few "mission-critical" information assets.

A fundamental problem, given the large volume of intelligence that one can gather about information security and the relatively time-consuming and tedious process of analysis, is being able to produce intelligence in a timely manner. Producing comprehensive, integrated intelligence across an enterprise will be a challenge at first, and a learning curve will be unavoidable. For the recommended ID-ISRMS to function properly, business stakeholders must form relationships among themselves that involve high levels of trust. These relationships will affect the usefulness of finished intelligence products, which is as dependent on the quality of the intelligence collected as it is on the analytical competence of the SPO. Also, the availability of good intelligence does not by any means guarantee good managerial decision making. One must consume, comprehend, and appropriately apply it; SA is an indispensable component of operational effectiveness but only insofar as it supports the knowledge and skill of the operator. Lastly, it is possible that the resources and powers available to the U.S. Intelligence community are more instrumental to intelligence cycle success than we realize.

One needs to validate the ID-ISRMS that we recommend in this paper by actually implementing it in an organization and then evaluating it for effectiveness and operational efficiency (e.g., in the course of an action research project). Our next step is to locate an organization willing to grant us access for this purpose.

References

Ab Rahman, A., Hidayah, N., & Choo, K.-K. R. (2015). A survey of information security incident handling in the cloud. *Computers & Security, 49*, 45-69.

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

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams—challenges in supporting the organizational security function. *Computers & Security, 31*, 643-652.

Ahmad, A., Maynard, S. B., Shanks, G. (2015). A case analysis of information systems and security incident responses. *International Journal of Information Management, 35*(6), 717-723.

Al-Ahmad, W., & Mohammad, B. (2012). Can a single security framework address information security risks adequately? *International Journal of Digital Information and Wireless Communications, 2*(3), 222-230.

Baker, W. H., Rees, L. P., & Tippett, P. S. (2007). Necessary measures: Metric-driven information security risk assessment and decision making. *Communications of the ACM, 50*(10), 101-106.

Baracaldo, N., & Joshi, J. (2013). An adaptive risk management and access control framework to mitigate insider threats. *Computers & Security*, *39*, 237-254.

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

Baskerville, R., & Pries-Heje, J. (2010). Explanatory design theory. *Business & Information Systems Engineering*, *2*(5), 271-282.

Coles, R. S., & Moulton, R. (2003). Operationalizing IT risk management. *Computers & Security*, *22*(6), 487-93.

Colwill, C. (2009). Human factors in information security: The insider threat—who can you trust these days? *Information Security Technical Report*, *14*(4), 186-196.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*(1), 90-101.

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196-207.

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, *49*, 162-176.

Endsley M. R. (1988). Design and evaluation for situation awareness enhancement. In *Proceedings of the Human Factors Society 32nd Annual Meeting* (pp. 97-101).

Endsley M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors*, *37*(1), 32-64.

Endsley, M. R., & Jones, D. G. (2011). *Designing for situation awareness: An approach to user-centered design.* London: CRC Press.

Enisa. (n.d.). *Inventory of risk management / risk assessment methods and tools*. Retrieved from http://rm-inv.enisa.europa.eu/methods

Fang, Y., Liang, Q., & Jia, Z. (2011). Knowledge sharing risk warning of industry cluster: An engineering perspective. In *Systems Engineering Procedia 2: Complexity System and Engineering Management* (pp. 412-421).

Feledi, D., Fenz, S., & Lechner, L. (2013). Toward Web-based information security knowledge sharing. *In Proceedings of the 7th International Conference on Availability, Reliability and* Security (pp. 199-209).

Fenz, S., Ekelhart, A., & Neubauer, T. (2009). Business process-based resource importance determination. *Lecture Notes in Computer Science, 5701*, 113-127.

Fenz, S. (2012). Increasing knowledge capturing efficiency by enterprise portals. *VINE: The Journal of Information & Knowledge Management Systems*, *42*(2), 237-250.

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security*, *22*(5), 410-430.

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, *43*, 90-110.

Friedberg, I., Skopik, F., Settanni, G., & Fiedler, R. (2015). Combating advanced persistent threats: From network event correlation to incident detection. *Computers & Security*, *48*, 35-57.

Gregor, S., & Jones, D. (2007). The anatomy of a design theory. *Journal of the Association for Information Systems*, *8*(5), 313-335.

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, *32*, 242-251.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28(*1), 75-105.

Hulme G. V. (2004). Getting at risk. In M. E. Whitma & H. J. Mattord (Eds.), *Management of information security* (pp. 307-308). Boston: Thomson Course Technology.

ISO. (n.d.). Management system standards. Retrieved from http://www.iso.org/iso/home/standards/management-standards.htm

ISO/IEC 27005:2011. (2011). *Information technology—security techniques—information security risk management.*

ISO 31000:2009. (2009). *Risk management—principles and guidelines.*

Jaatun, M. G., Albrechtsen, E., Line, M. B. Tøndel, I. E., & Longva, O. E. (2009). A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection*, *2*(1), 26-37.

Kowalski, E., Cappelli, D., & Moore, A. (2008). *Insider threat study: Illicit cyber activity in the information technology and telecommunications sector*. Washington, DC: Software Engineering Institute and United States Secret Service.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management*, *41*, 597-607.

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

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems, 15*(4), 251-266.

Matwyshyn, A. (2009). CSR and the corporate cyborg: Ethical corporate information security practices. *Journal of Business Ethics*, *88*(S4), 579-594.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, *18*(2), 126-139.

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management*, *52*(1), 123-134.

Neuman, W. L. (2011). *Social research methods: Qualitative and quantitative approaches*. Boston, Massachusetts: Allyn & Bacon.

Nunamaker, J. F., Jr., Chen, M., & Purdin, T. D. M. (1990). Systems development in information systems research. *Journal of Management Information Systems, 7*(3), 89-106.

Parker, D. B. (2007). Risks of risk-based security. *Communications of the ACM*, *50*(3), 120.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165-176.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45-77.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*, 597-611.

Qian, Y., Fang, Y., & Gonzalez, J. J. (2012). Managing information security risks during new technology adoption. *Computers & Security*, *31,* 859-869.

Raiu, C. (2012). Cyber-threat evolution: The past year. *Computer Fraud & Security*, *3*, 5-8.

Reece, R. P., & Stahl, B. C. (2015). The professionalisation of information security: Perspectives of UK practitioners. *Computers & Security*, *48*, 182-195.

Rees J., & Allen, J. (2008). The state of risk assessment practices in information security: An exploratory investigation. *Journal of Organizational Computing and Electronic Commerce*, *18*(4), 255-277.

Rousseau, R., Tremblay, S., & Breton, R. (2004). Defining and modeling situation awareness: A critical review. In S. Tremblay & S. Banbury (Eds.), *A cognitive approach to situation awareness: Theory and application* (pp. 3-21). Burlington: Ashgate Publishing Company.

Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic optimism on information security management. *Computers & Security*, *31*, 221-232.

Ruighaver, A. B., Maynard, S. B., & Warren, M. (2012). Ethical decision making: Improving the quality of acceptable use policies. Computers & Security, *29*(7), 731-736.

Schmittling R. (2010) Performing a security risk assessment. ISACA Journal, *1*, 1-7.

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

Shedden, P., Scheepers, R., Smith, W., & Ahmad, A. (2011). Incorporating a knowledge perspective into security risk assessments. *VINE: The Journal of Information & Knowledge Management Systems*, *41*(2), 152-166.

Shedden, P., Ahmad, A., Smith, W., Tscherning, H., & Scheepers, R. (2016). Asset identification in information security risk assessment: A business practice approach. *Communications of the Association for Information Systems*, *39*(1), 15.

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM*, *49*(8), 97-100.

Stewart G., & Lacey, D. (2012). Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management & Computer Security*, *20*(1), 29-38.

Tamjidyamcholo, A., Baba, M. S. B., Shuib, N. L. M., & Rohani, V. A. (2014). Evaluation model for knowledge sharing in information security professional virtual community. *Computers & Security, 43*, 19-34.

Tamjidyamcholo, A., Baba, M. S. B., Tamjid, H., & Gholipour, R. (2013). Information security—professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language. *Computers & Education, 68*, 223-232.

Tamjidyamcholo, A., & Al-Dabbagh, R. D. (2012). Genetic algorithm approach for risk reduction of information security. *International Journal of Cyber-Security and Digital Forensics, 1*(1), 59-66.

Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security*, *45*, 42-57.

Treverton, G. F., Jones, S. G., Boraz, S., & Lipscy, P. (2006). Toward a theory of intelligence. In *Proceedings of the RAND National Security Research Division Workshop.*

Utin, D. M., Utin, M. A., & Utin, J. (2008). General misconceptions about information security lead to an insecure world. *Information Security Journal: A Global Perspective*, *17*(4), 164-169.

Venable, J. R. (2013). Rethinking design theory in information systems. In. J. vom Brocke, R. Hekkala, S. Ram, & M. Rossi (Eds.), *DESRIST 2013* (LNCS 7939, pp. 136-149). Berlin: Springer.

Venable, J., Pries-Heje, J., & Baskerville, R. (2014). FEDS: A framework for evaluation in design science research. *European Journal of Information Systems*, *25*(1), 77-89.

Von Grebmer, A. (2007). *Information and IT risk management in a nutshell: A pragmatic approach to information security*. Norderstedt, Germany: Books on Demand.

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *23*, 191-198.

Walls, J. G., Widmeyer, G. R., & El Sawy, O. A. (1992). Building an information system design theory for vigilant EIS. *Information Systems Research*, *3*(1), 36-59.

Werlinger, R., Muldner, K., Hawkey, K., Beznosov, K. (2010). Preparation, detection, and analysis: The diagnostic work of IT security incident response. *Information Management & Computer Security*, *18*(1), 26-42.

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

Whitman, M. E., & Mattord, H. J. (2012). Threats to information security revisited. *Journal of Information System Security*, *8*(1), 21-41.

Young, R., & Windsor, J. (2010). Empirical evaluation of information security planning and integration. *Communications of AIS, 26*, 245-266.

About the Authors

Jeb Webb is a PhD student at the Department of Computing and Information Systems, University of Melbourne. He received a Bachelor of Arts in Political Science from the University of California at Berkeley and a Master of Arts in Intelligence Studies (Information Warfare concentration) from American Military University. He is a veteran of the U.S. Army special operations community with service in an intelligence support capacity.

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. Heis 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.

Sean B. Maynard is an academic based at the Department of Computing and Information Systems, University of Melbourne. Starting his academic career in Information Systems focusing on the use of computing technology to aid senior management (EIS) and the evaluation of decision support systems, his research over the past two decades has been in the area of information security, in particular focusing on the evaluation of security policy quality and on the investigation of security culture within organizations.

Graeme Shanks is a Professor of Information Systems in the Department of Computing and Information Systems at the University of Melbourne. His research interests include business analytics, the implementation and impact of information systems, data quality, conceptual modeling and case study research in information systems. Graeme has published widely in information systems journals and conferences. He is a member of the editorial boards of several journals and was recently a member of the Australian Research Council College of Experts.

JITTA

JOURNAL OF INFORMATION TECHNOLOGY THEORY AND APPLICATION

JITTA is a Publication of the Association for Information Systems
ISSN: 1532-3416