Towards an Intelligence-Driven Information Security Risk Management Process for Organisations

Jeb Webb
Sean Maynard
Atif Ahmad
Graeme Shanks
Department of Computing and Information Systems
Melbourne School of Engineering
University of Melbourne
Victoria, Australia
Email: sean.maynard@unimelb.edu.au

Abstract

Three deficiencies exist in information security under prevailing practices: organisations tend to focus on compliance over protection; to estimate risk without investigating it; and to assess risk on an occasional (as opposed to continuous) basis. These tendencies indicate that important data is being missed and that the situation awareness of decision-makers in many organisations is currently inadequate. This research-in-progress paper uses Endsley's situation awareness theory, and examines how the structure and functions of the US national security intelligence enterprise—a revelatory case of enterprise situation awareness development in security and risk management—correspond with Endsley's theoretical model, and how facets of the US enterprise might be adapted to improve situation awareness in the information security risk management process of organisations.

Keywords

Information, Security, Risk Management, Enterprise Situation Awareness, Intelligence

INTRODUCTION

The modern organisation is essentially built of information: almost everything the organisation is and does involves information's storage, use, or communication. *Information security* is a broad term that essentially refers to the practice of protecting information and the ways in which it is used to serve the goals of an organisation (Whitman and Mattord 2004). Given the supreme role of information in the functions of organisations, the importance of information security is widely acknowledged (Baskerville 1991; Shedden et al. 2010). Laws and standards designed to guide information security practices have become more prevalent worldwide. These laws and standards typically endorse a "risk management" approach to information security. The object of risk management is to identify sources of risk and deal with them appropriately. Managing information security risks effectively, however, requires accurate appraisal of the organisation's overall information security situation, and there is evidence that, under prevailing practices, much of the information required to model risk representatively is simply not being incorporated into organisations' information security risk assessments (Parker 2007; Shedden et al. 2011; Shedden et al. 2010; Utin et al. 2008).

A review of information security literature revealed that organisations tend to focus on compliance over protection (Johnson 2009; Matwyshyn 2009; Shedden et al. 2010; Young and Windsor 2010); to estimate risk rather than investigating it (Parker 2007; Richardson 2011; Shedden et al. 2011; Utin et al. 2008); and to assess risk on an occasional—as opposed to continuous—basis (Rees and Allen 2008; Schmittling 2010; Hulme 2004). Each of these tendencies describes a way in which important security status information is being omitted from Information Security Risk Management (ISRM) decision making. The decisions that senior managers need to make relating to their organizations' information security postures (e.g. whether to change the way the organization does things to avoid negative situations that could cost it money, damage its reputation, or otherwise impede its accomplishment of strategic objectives) need to be informed by accurate understanding of the risks their *particular* organizations are actually faced with.

We argue that this problem can be described as one of leaders and their subordinates lacking situation awareness in regard to the security states of their organizations. The decision-makers in many organizations are neither

registering how developments within their operational environments affect the security of their information and information systems, nor recognizing how the functionality and strategic interests of the organization as a whole are contingent upon this security. This research-in-progress paper is part of a research project which aims to develop an intelligence-driven ISRM process that maximizes situation awareness among the decision-makers involved in that process. In this initial stage of the project we use a document-based case study to identify whether Endsley's situation awareness model can be utilized at an organisation level. Ultimately, our aim is to answer the following research question:

"How can situation awareness be increased in information security risk management?"

This research-in-progress paper is organized as follows. The background to the study is discussed including the literature on information systems security and an introduction of Endsley's situational awareness model (1995). Next the research approach for the research is presented. Following this, a document-based case study is presented in which Endsley's model is used to develop an *a priori* version of the ISRM model. We conclude this research-in-progress paper with a discussion of the project's outlook and its potential implications/contributions.

BACKGROUND

This section reviews two relevant literature areas. It first examines work in information security risk assessment. Secondly, it discusses situational awareness, in particularly Endsley's model of situational awareness.

Information Security and Risk Assessment

In the literature on information security risk management practices three apparently endemic deficiencies were uncovered: (1) Security risk assessment is aimed at compliance rather than protection; (2) Security risks are estimated without investigation; and (3) Security risk is not assessed historically and continuously.

Security risk assessment is aimed at compliance rather than protection

Many organisations treat compliance with laws and standards as ends rather than means (e.g. Johnson 2009; Matwyshyn 2009; Shedden et al. 2010; Young and Windsor 2010). Neither the technical fulfilment of legal obligations nor the perception of having fulfilled a standard is the same as achieving information security, however (Matwyshyn 2009; Shedden et al. 2010, von Grebmer 2006). Laws and standards are generic by design and their provisions are consequently vague (Broderick 2006; Siponen 2006; Siponen and Willison 2009). An organisation's unique and dynamic situation cannot be addressed by laws or standards alone (Baskerville 1991). An organisation can be deemed 100 percent compliant under conventionally accepted standards without having actually achieved a state of information security (von Grebmer 2006). When compliance with externally formed ideals is held to be the goal, protection may be assured theoretically, but it is not assured actually.

Security risks are estimated without investigation

Whilst the existence of standards and legal requirements reinforces the message that information security is important, the degree to which information security is unique to each organisation appears to be widely misunderstood (Parker 2007; Richardson 2011; Shedden et al. 2011; Utin et al. 2008). Standardized approaches to risk estimation are rarely useful toward estimating the specific risks that a particular organisation is faced with. Rather, these methods lead practitioners to settle on guessed values and imagined probabilities virtually *prima facie* (Baskerville 1991). Nevertheless, such approaches are commonly accepted by many organisations as adequate means for managing information security risk (Parker 2007; Utin et al. 2008). Risk cannot be properly managed unless it is fully understood (Humphreys 2008). To understand information security risk fully, organisations must ensure that the roles and characteristics of the information assets their business processes depend on are understood through ongoing, conscientious investigation, and that lessons learned become matters of record.

Security risk is not assessed historically and continuously

Many organisations conduct information security risk assessments as infrequent events occurring somewhere between quarterly and yearly (Rees and Allen 2008). When carried out this way, a detailed assessment can become overwhelming because all of the pertinent information must be gathered within a limited time frame.

Furthermore, information gathered at any one point in time only constitutes a status "snapshot" of the organisation's actually fluid information security environment (Schmittling 2010). Hulme notes that "A risk assessment conducted on the first day of the month can be quite different than the same assessment conducted several weeks later;" and that risk can be most effectively minimized by keeping "eternally vigilant" (2004). Ahmad, Hadgkiss and Ruighaver (2012) argue that it is also important for organisations to retain memory of past security incidents and identified problem indications. In their failure to remain attentive and retentive, many organisations are missing out on vital risk-pertinent data about current developments and long-term trends that could afford them advance warning, by means of predictive analysis, of impending incidents.

Summary of risk assessment deficiencies

Each of the three flaws outlined above describes a way that important information about risk is misapprehended or simply missed altogether. Without this information, managers' understandings of their organisations' security situations are fragmentary. We argue that this problem can be described as one of leaders and their subordinates lacking *situation awareness* concerning the security states of their organisations.

The phenomenon known as situation awareness (SA), as it is explained by Endsley's (1995) SA theory, occurs when an actor, whose function is to decide and act appropriately on (or in response to) a situation, has the relevant status information he or she requires about the elements of (i.e. the "different things going on" within) this situation of interest to decide and act appropriately. As SA theory describes how decision-making actors come to understand the contexts within which they function, we argue that it is an appropriate theory for the current project, which aims to increase information security risk managers' awareness of their organizations' respective security situations.

Theoretical basis: Endsley's theory of situation awareness

Mica Endsley's theory of SA is by far the most widely accepted and validated theory of SA (Salmon 2008). While other authors have modelled some aspects of SA differently, or have argued that an SA theory should draw on theoretical underpinnings different from those Endsley has drawn upon, a review of the literature failed to uncover any arguments that genuinely undermine the validity of her theory or that offer better—or, we would argue, even significantly different—explanations of how people come to develop awareness of situational states in the context of goal-oriented activities.

Endsley defines SA 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 1988, in Endsley and Jones 2011). In Endsley's model, SA is achieved in progressive stages. In Level 1 SA, one perceives, or becomes aware of, "the status, attributes, and dynamics of relevant elements in the environment" (Endsley 1988, in Endsley and Jones 2011). Failure to achieve Level 1 SA essentially amounts to a failure to perceive relevant information about the environment, given one's information requirements in light of one's goals and objectives. In Level 2 SA, one compares perceptions of the environment against one's internally held understanding of, or associations regarding, this incoming information ("prototypical situations in memory;" Endsley 1995). Failure to achieve Level 2 SA amounts to a failure to understand what has been perceived, which can stem from information overload or from having inadequate informational templates (e.g. "mental models" held in human memory) to reference in processing and interpreting the sensed/incoming information (Endsley 1995). When Level 2 SA is achieved, one is aware of information's intrinsic meaning(s), as well as its significance in the context of functional goals and objectives.

Level 3 SA occurs when one is able to extrapolate the implications of things perceived about the environment, to predict what will happen "at least in the very near term," based on one's extant understanding of cause and effect relationships between the elements of a situation (Endsley 1995). To achieve Level 3 SA, one must already have developed Level 2 SA. Level 3 SA enables one to anticipate and plan for alternative future scenarios. Failure at this level can stem from information overload or inadequate subject matter knowledge (Endsley and Jones 2011). Endsley's model portrays SA as a phenomenon that occurs in the context of decision-making, as it recognizes SA to be purposeful or goal oriented: "Goals form the basis for most decision making in dynamic environments" (Endsley 1995). What we might call "high fidelity" Level 3 SA, or Level 3 SA borne out of assessing the situation of interest accurately, and interpreting it rationally in the context of goals and objectives, becomes the basis for informed decision making (Endsley and Jones 2011). Endsley's model of SA is depicted in Figure 1.

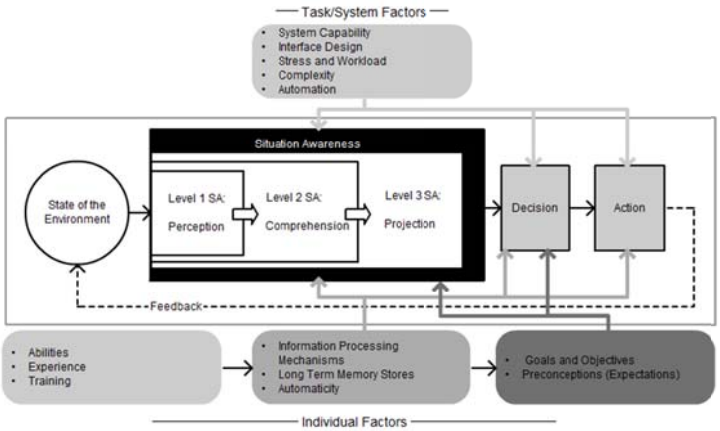

Figure 1: Endsley's Situation Awareness Model (Adapted from Endsley 1995)

Above and below the chain from perception to action upon a situation (grouped into coloured boxes in Figure 1) are task/system and individual factors that bear on the SA development and decision making processes. All of these factors only become meaningful in the context of a specific individual or system. As our project concerns coordinated or "team" SA development, however, the roles of "goals and objectives"—which are shared between team members—have special relevance and are ultimately singled out for representation in our adapted model. Endsley explains that SA within a team involves "a specific set of SA elements" for each member, pertinent to his or her functions within the team, with some overlapping between these elements (Endsley 1995). Overlapping occurs where goals and objectives are shared between team members. Similarly, any member may acquire information that meets the SA needs/requirements of another member and, in such a case, this information should be shared (Endsley 1995). Endsley defines the SA of the team as "the degree to which every team member possesses the SA required for his or her responsibilities" (Endsley 1995).

RESEARCH APPROACH

This is a design science research project employing mixed qualitative analytical methods. The overall project's design comprises the following phases: (1) a literature review to identify a gap/need in the information security subject area; (2) adaptation of Endsley's theoretical model of SA to include supported second-party decision making; (3) a single case revelatory case study (Yin 2009) in which open source documents were textually analysed and coded (Carley 1993; Neuman 2011) to determine whether the functions of the USNSIE correspond with the adapted model; (4) the specification of an *a priori* model for an ISRM process in particular, based on findings from the literature review and logical analogues between US national security intelligence enterprise components and the components of typical organisations; (5) expert interviews with information security risk managers to validate or revise components of the *a priori* model; (6) the specification of a revised model based on expert input; and (7) focus groups to refine and validate the revised model. Of these 7 phases, 1-4 have been completed.

Case study of the US national security intelligence enterprise: enterprise SA production

We argue that the US stands as the world's richest organisation in terms of both its wealth and the complexity of its critical national infrastructure. Its national security intelligence enterprise represents perhaps the ultimate example of SA in the interest of asset protection. The US Intelligence Community (IC) is composed of 17 specialised but coordinated elements dedicated to collecting and processing information required by decision-makers to establish awareness vis-à-vis national security issues (ODNI 2011). As the US National Security Intelligence Enterprise (USNSIE), which comprises the US IC and the military and governmental decision-makers that the IC serves, describes an SA enterprise devoted to informing the management of risks to national security, we argue that the USNSIE provides a revelatory case of how SA can be achieved across a security risk management enterprise. The object of the case study was to understand how the USNSIE develops SA and facilitates the SA of decision makers in government; the purpose of doing this was to derive a process model for enterprise SA development. The case study involved the analysis of 71 documents. The documents analysed included US law, IC policy documents (Intelligence Community Directives or "ICDs"), military manuals and other US Government publications, US Government websites, and authoritative works produced by subject matter experts.

Initially, open coding (Neuman 2011) was carried out on 32 ICDs and 5 pieces of US legislation to compile a lexical concordance of named actors and functions (Carley 1993). The concordance was constructed, using Microsoft Word, in the form of a large (171pages) table consisting of 154 entries. ICDs and legislation were selected for analysis based on their titles and apparent themes. Axial coding followed open coding. The object of axial coding is to evaluate previously developed codes for their utility in describing themes of interest within the study (Neuman 2011). We realized that the vast majority of the data we had collected concerned details that—though they concerned the structure of the USNSIE at the highest strategic level—were still too specific (and complex) for adaptation into analogue components for a realistic organizational ISRM process model. Furthermore, while we now had a fair idea of the USNSIE's structure and role in government, our understanding of how intelligence is actually created and disseminated within this enterprise was still lacking.

A search of available literature revealed that no theory has been accepted as a definitive explanation of the process by which a national security intelligence enterprise informs decision making (Treverton et al. 2006). Typically, the overall process of identifying the intelligence needs of decision-makers and carrying out the operations required to meet these needs is described in terms of a conceptual framework known as the "intelligence cycle" (Johnson 2012). The intelligence cycle is a feedback loop divided into phases of activity. The number of discrete phases composing this cycle is a matter of opinion and varies across authors. We argue that the intelligence cycle is most accurately depicted as a twelve phase cycle, as this allots a discrete phase for each component activity. While the intelligence cycle is a useful heuristic for understanding how intelligence generally informs decision making, it does not in itself constitute a detailed process description, however. Thus, our next step was to assemble a suitable process description.

We created an outline of the intelligence cycle in which each phase represented the heading of a section. We then reviewed the entries of the actors and functions table to determine the most key/central actors at the highest enterprise levels. Next, we constructed a step-by-step account of what happens within the USNSIE throughout the intelligence cycle. As we drafted this account, its components were considered for their overall representativeness, centrality, and level of granularity within the USNSIE: actors that were too specific to the peculiar functions of the enterprise, or which served less than central functions, were considered poor candidates for adaptation into a high level process model and were omitted from our account on that basis. Essentially, this phase consisted of multiple iterations of selective coding, during which data was reorganized under themes to further inform our understanding of "major themes or concepts" of interest (Neuman 2011).

At this stage we still lacked a robust theoretical template on which to propose a process model. A search for theory relating to the role of situation awareness in decision making and action ultimately led us to Mica Endsley's SA theory. To determine whether Endsley's theoretical model of SA could be used to describe the USNSIE, we then applied the pattern matching variation of the illustrative method (Neuman 2011). Neuman explains that the illustrative method involves deriving "empty boxes" from components of pre-existent theory and then filling these boxes with findings from research data (2011). In our case, these "empty boxes" were structural components of Endsley's theoretical model, which we "filled" with case study data. We compared concepts within SA theory (i.e. task and system factors, stages of SA development, decision and action phases, and its feedback loop) to the phases of the intelligence cycle to identify points of analogy. We then sought to adapt Endsley's model to better describe the way a team of actors can serve as "purveyors of situation awareness" to decision makers the context of an intelligence enterprise.

This involved successive approximation, described by Neuman as "(a) method of qualitative data analysis that repeatedly moves back and forth between the empirical data and the abstract concepts, theories, or models, adjusting theory and refining data collection each time" (2011). Evidence from the case study was considered and reconsidered within the context of Endsley's SA-development/decision/action cycle to yield a process template describing enterprise SA production in support of a single decision making actor. Figure 2 illustrates how the intelligence cycle framework can be represented as an adapted situation awareness process model. The process of developing SA, whether it is confined to individual experience or applied to a distributed enterprise, describes the organisation and interpretation of situational element status data into an overall understanding of a situation. While Endsley's model of individual SA pertains to an individual acting directly upon or in response to a situation, Figure 2 portrays SA development through the concerted effort of multiple actors whose overall function is to develop and then export this SA to a consumer who then acts (or directs action) on or in response to the situation of interest. In Figure 2, US IC actors have been simplistically divided into two types: collection components and analysis components. Table 1 maps correspondences between the intelligence cycle and SA theory.

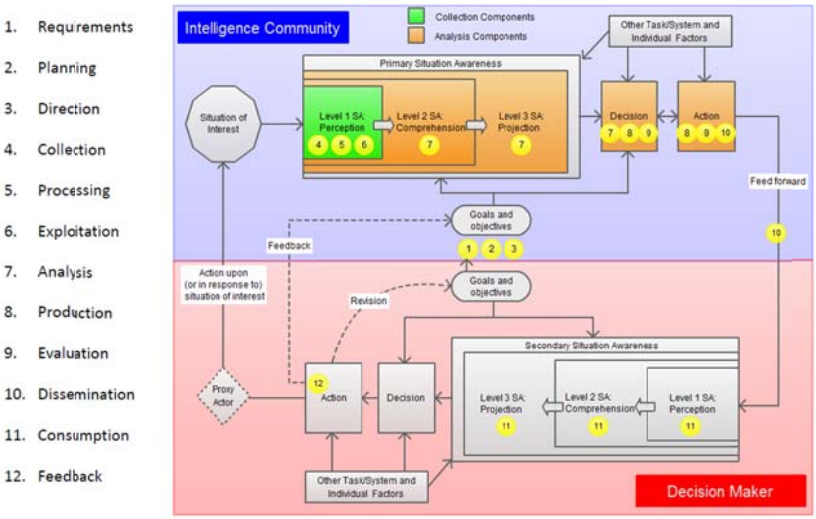

Figure 2: Enterprise SA in the Context of the Intelligence Cycle

Table 1: Correspondences between the Intelligence Cycle and SA Theory

Intelligence Cycle Phases 1, 2 and 3: Requirements, Planning, and Direction	SA Theory Analogue Goals and Objectives
Explanation The goals and objectives of decision-makers determine intelligence requirements. These requirements are then translated into operational requirements at the IC element level (ICD 900; JP 2-0). In phases 2 and 3, planning and direction by IC leadership determines the goals and objectives of operators within IC elements (ODNI 2011). These goals and objectives provide the context by which situational element states are judged—determining what needs to be perceived and why, and informing understanding of developments' implications, given the goals and objectives of the decision-making intelligence consumer (ODNI 2011).	
Intelligence Cycle Phases 4, 5, and 6: Collection, Processing, and Exploitation	SA Theory Analogue Level 1 SA (Perception)
Explanation: During collection, situational element state data is gathered by human or technical assets (Johnson 2012; JP 2-0). Perception occurs when element states are perceptible by conscious agents (Endsley 1995). In human assets, collection and processing can occur concurrently; human perception of technical data occurs after some machine processing (JP 2-0; Miller 2004). Exploitation requires basic relevance recognition and is often automated to some extent (JP 2-0; ICD 300; ODNI 2011). Humans facilitate exploitation by labelling and classifying information for easy discovery or by forwarding information where useful (Miller 2004; ODNI 2011).	
Intelligence Cycle Phase 7: Analysis	SA Theory Analogues Level 2 SA (Comprehension); Level 3 SA (Projection); Decision
Explanation Situational comprehension occurs at the analysis phase of the intelligence cycle (Katter, Montgomery and Thompson 1979). Analysis can focus on anywhere from current to long term situations, and often draws on the expertise of multiple specialist analysts to develop multidimensional comprehension of a particular situation (JP 2-0). Analysts are commonly expected to apply their knowledge in the subject area to anticipate the implications of a situation's current status, and its likely future state, for decision-makers' goals and objectives (USG 2009). Analysts decide and act across analysis, production, evaluation and dissemination.	
Intelligence Cycle Phase 8: Production	SA Theory Analogues Decision; Action
Explanation The process of creating a coherent piece of finished intelligence explaining the analyst's findings, rationale, limitations, recommendations, etc., is referred to as "production;" the finished intelligence, which can be in any media format, is often referred to as an "intelligence product" (ODNI 2011). The analyst must make decisions that amount to findings as well as decisions about how to communicate these findings in the final product, given the stated needs of the consumer.	
Intelligence Cycle Phase 9: Evaluation	SA Theory Analogues Decision; Action
Explanation The analyst, and under some circumstances the analyst's superior, must also carry out an evaluation of the intelligence product, to verify that it fulfils the consumer/decision-maker's stated intelligence requirements, prior to the product's dissemination (ICD 203). Both production and evaluation can involve reiterations of decision and action when products are evaluated negatively (JP 2-0; ICD 203).	
Intelligence Cycle Phase 10: Dissemination	SA Theory Analogue Action
Explanation The action of disseminating a useful and appropriate intelligence product is the ultimate functional objective of the intelligence analyst (Treverton and Gabbard 2008). Intelligence products may be disseminated physically, electronically, presented formally or simply communicated, depending on the type of intelligence involved, consumer needs and specifications, and temporal, locational, or other practical considerations (ODNI 2011).	
Intelligence Cycle Phase 11: Consumption	SA Theory Analogue Level 1 SA (Perception); Level 2 SA (Comprehension); Level 3 SA (Projection)

Explanation The disseminated product is consumed (listened to, read, or otherwise perceived) by the decision-maker (ODNI 2011). Consumption initiates the process of SA synthesis in the mind of the consumer. Consumed intelligence is not always passively assimilated; the decision-maker often compares the product's contents to information held in memory to develop personal understanding of the situation (Lowenthal 2000). While perception and lower level comprehension may occur in rapid succession, higher level comprehension of the situation and the internal formation of projections by the decision-maker may require a period of reflection and rumination.	
Intelligence Cycle Phase 12: Feedback	SA Theory Analogue Action
Explanation In the context of the intelligence cycle, feedback refers to the decision-maker's confirmation or denial, to an IC liaison, that the intelligence product has met his or her stated information requirements regarding the situation of interest (ODNI, 2011). It is an action by the decision-maker that is inherent to the cycle itself.	

Though integral to the USNSIE, issuing feedback is not, of course, the decision-maker's definitive function. The role of the decision-maker is to make decisions that lead to action on, or in reaction to, a situation of interest, as necessary in light of strategic goals and objectives. If the incoming intelligence suggests that a situation requires action, then the decision-maker will make a decision concerning what action is required and, to some extent, how it should be carried out. In many cases, the decision-maker in government does not carry out an action but rather directs one or more proxy actors to do so (Johnson 2012; Lowenthal 2000). Alternatively, if intelligence suggests that the situation is already conducive to the goals and objectives of the decision-maker, action may not be required. Yet another possibility is that the intelligence presents the situation differently than the decision-maker had previously conceived of it, and the decision-maker must revise his or her goals and objectives to accommodate this new understanding (Lowenthal 2000). If action affecting the relative state of the situation is carried out by the decision-maker or proxy, the situation changes and a new enterprise SA development and synthesis process must be undertaken by the US IC and the decision-maker to establish current awareness of it.

DISCUSSION

In the previous section, we have argued that the USNSIE is actually an example of enterprise SA. We will now argue that this enterprise model can be applied toward the design of a situation-aware ISRM process for organizations. Just as an enterprise consists of layered activities, enterprise SA must also be considered at multiple levels. In Figure 2, the combined efforts of the entire intelligence community have been simplified into one tier of a two-tiered model. While this may accurately depict the nature of the enterprise at a high level, the reader must remember that the model can be adapted to describe any transaction in which SA is developed by an actor or team of actors and provided to another actor who then decides and acts in response to the situation of interest. This is to say that the model can be adapted to describe activity between all layers of the SA enterprise.

In the next section we present an adapted, *a priori* model describing a situation-aware/intelligence-driven ISRM process at the business process level. It is the second of three diagrams (depicting [1] transactions between department level collection and analysis assets and business process owners; [2] transactions between business process owners and the ISRM Manager; and [3] transactions between the ISRM Manager and an executive level officer, such as a Chief Information Security Officer, or Chief Security or Risk Officer, where such a relationship exists within the hierarchy of an organization) that have been developed to describe the proposed process. The others have been omitted from this paper due to space considerations.

An *a priori* model for intelligence-driven ISRM

We propose that enterprise SA development in ISRM should start with collection and analysis at the department level. The departments are intrinsically specialized to carry out particular functions within the organisation, and should be most familiar with the information assets located under their respective functions. Responsibility for ISRM should be distributed across business process owners (Coles and Moulton 2003), who have tasking authority over collection and analysis components embedded within the departments. The business process owners report up to the ISRM head, subordinate to the organisation's risk or security executive (where one exists).

At the department level, the security statuses of specific information assets are the collection targets. If multiple information assets that fall under the same department are interdependent or otherwise interact with each other, the department-level intelligence component is responsible for collecting status information relating both to the separate information assets as well as to their interactions between each other. "Information assets" includes pieces of hardware, software, network assets, individual people, specific procedures, and data assets (Whitman and Mattord 2004).

While the security states of hardware, software, and network assets generally fall under the purview of the organisation's IT department regardless of the business process concerned, other information assets supporting a business process, such as the people, procedures and pieces of information involved, may be distributed across

several departments. Collection targets should be developed with guidance from the enterprise and business process levels in the form of refined and prioritized intelligence requirements. Intelligence forwarded from departmental collection and analysis components is received and aggregated by business process owners, who then perform business process level analyses. The products resulting from these analyses are then disseminated upward to the ISRM head, who aggregates the findings to perform a whole-enterprise security assessment.

Figure 3 depicts our *a priori* model of intelligence-driven ISRM at the business process level. The diagram illustrates the relationship between each business process owner and the Information Security Risk Manager. The relationship between *all* business process owners and the manager can be similarly modelled, however, in much the same way as the upper tier of Figure 2 represents the combined efforts of US IC components. In Figure 3, authority to act on a process level situation is generally delegated to the business process owner, subject to oversight by the ISRM Manager. A similar diagram applies to the relationships between department level collection and analysis assets and each business process owner, wherein the department level assets assume the upper tier of the diagram, the business process owners assume the lower tier, and authority to act on a department level situation is held by the business process owner(s) involved, but may be delegated to an actor at the department level.

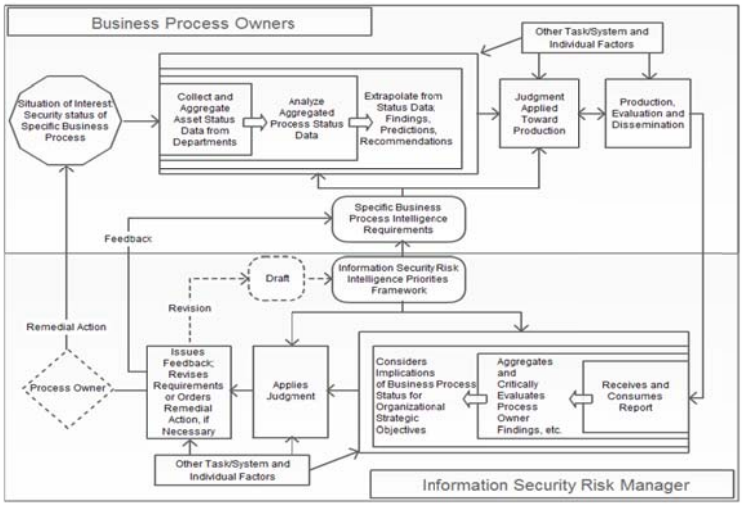

Figure 3: Intelligence-Driven ISRM at the Business Process Level

CONCLUSION

This research-in-progress paper has discussed the development of an intelligence-driven ISRM process model for organisations. It has described three types of SA deficiencies identified in information security literature and proposes an enterprise SA model, derived from a case study of the USNSIE, to improve SA in ISRM. The next step for this research project will be to conduct interviews with subject matter experts from the ISRM field. The point of these interviews will be to elicit expert advice concerning the general feasibility of the *a priori* model as presented here, as well as general, high level recommendations for improving it. Following incorporation of this input, we will then present the resulting model to a focus group. While the purpose of the initial expert interviews will be to determine what components—if any—of the model are considered valid propositions in the broad sense, the purpose of the focus groups will be to revise, refine, and validate lower level components of the formerly validated high level model.

The intelligence driven ISRM process model has several important implications for practitioners and researchers. First, it will enable more accurate estimations of risk in information security by distributing the assessment workload across the enterprise, rendering more detailed assessments practicable. Second, it will institute continuous monitoring and reporting/documentation practices, increasing the chances of threat detection while also enabling trend mapping and predictive analysis. The net result of this for practitioners will be better-informed decision-making in ISRM at both the business process and whole enterprise levels. As the model approaches ISRM from a business process security perspective, it links ISRM directly to the strategic business interests of the organisation, increasing the likelihood of enthusiastic support by upper management.

The model will also provide the basis for further research in situation-aware/intelligent information security risk management. The model should ultimately be developed into a complete method that guides organizations through the process of SA/intelligence requirements identification, as well as through ISRM-specific collection and analysis procedures. Empirical work needs to be done to evaluate the actual feasibility of the model and any resulting method. Action research studies implementing ISRM methods based on the model resulting from this project would be particularly useful.

REFERENCES

Ahmad, Atif, Justin Hadgkiss, and A.B. Ruighaver. 2012. "Incident response teams – Challenges in supporting the organisational security function." *Computers & Security* 31, 643-652.

Baskerville, R. 1991. "Risk Analysis: an interpretive feasibility tool in justifying information systems security." *European Journal of Information Systems* 1, no.2: 121-130.

Broderick, J. Stuart."ISMS, Security Standards and Security Regulations." *Information Security Technical Report* 11, 26-31.

Carley, Kathleen. 1993. "Coding Choices for Textual Analysis: a Comparison of Content Analysis and Map Analysis." *Sociological Methodology* 23, no. 1: 75-126

Coles, Robert S., and Rolf Moulton. 2003."Operationalizing IT risk management." *Computers & Security* 22.6: 487-493

Director of National Intelligence. *Intelligence Community Directive Number 116: Intelligence Planning, Programming, Budgeting, and Evaluation System.* Washington, D.C.: Office of the Director of National Intelligence, 2011.

Director of National Intelligence. *Intelligence Community Directive Number 200: Management, Integration, and Oversight of Intelligence Community Analysis*. Washington, D.C.: Office of the Director of National Intelligence, 2007.

Director of National Intelligence. *Intelligence Community Directive Number 203: Analytic Standards.* Washington, D.C.: Office of the Director of National Intelligence, 2007.

Director of National Intelligence. *Intelligence Community Directive Number 300: Management, Integration, and Oversight of Intelligence Collection and Covert Action*. Washington, D.C.: Office of the Director of National Intelligence, 2006.

Director of National Intelligence. *Intelligence Community Directive Number 900: Mission Management*. Washington: Office of the Director of National Intelligence, 2006.

Endsley, M.R. 1988. "Design and Evaluation for Situation Awareness Enhancement." *Proceedings of the Human Factors Society 32nd Annual Meeting*, 97-101. Santa Monica, California: Human Factors Society.

Endsley, M.R. 1995. "Toward a Theory of Situation Awareness in Dynamic Systems." *Human Factors* 37, no. 1: 32-64.

Endsley, Mica R. and Debra G. Jones. 2011. *Designing for Situation Awareness: an Approach to User-Centered Design.* Boca Raton, Florida; London: CRC Press.

Hulme, George V. "Getting at Risk." In *Management of Information Security*, by Michael E. Whitman and Herbert J. Mattord, 307-308. Boston: Thomson Course Technology, 2004.

Humphreys, Edward. 2008. "Information security management standards: Compliance, governance and risk management." *Information Security Technical Report* 13, no. 4: 247-255.

Johnson, Alice M. 2009. "Business and Security Executives Views of Information Security Investment Drivers: Results from a Delphi Study." *Journal of Information Privacy & Security* 5, no. 1: 3-27.

Johnson, Loch K. 2012. *National Security Intelligence: Secret Operations in Defense of the Democracies*. Cambridge, UK; Malden, MA.

Joint Chiefs of Staff. *Joint Publication 2-0: Joint Intelligence*. Washington, D.C.: Office of the Joint Chiefs of Staff, 2007.

Katter, Robert V., Christine A. Montgomery, and John R. Thompson. 1979. "Human Processes in Intelligence Analysis." *Research Report 1237*. US Army Research Institute for the Behavioral and Social Sciences, US Army Intelligence and Security Command.

Lowenthal, Mark M. 2003. *Intelligence: From Secrets to Policy*. Washington, D.C.: CQ Press.

Matwyshyn, Andrea. 2010. "CSR and the Corporate Cyborg: Ethical Corporate Information Security Practices." *Journal of Business Ethics* 88, 579-594.

Miller, J.O. 2004. “Modeling the US Military Intelligence Process.” Department of Operational Sciences, Air Force Institute of Technology. Wright Patterson, OH.

Neuman, William Lawrence. 2011. *Social Research Methods: Qualitative and Quantitative approaches.* Boston, Massachusetts: Allyn & Bacon.

Office of the Director of National Intelligence. 2011. *US National Intelligence: an Overview*. Intelligence Consumer’s Guide. Washington, DC.

Parker, Donn B. 2007. "Risks of Risk-Based Security." *Communications Of The ACM* 50, no. 3: 120.

Rees, J, and J Allen. 2008. "The State of Risk Assessment Practices in Information Security: An Exploratory Investigation." *Journal of Organisational Computing and Electronic Commerce* 18, no. 4: 255-277.

Richardson, Robert. 2011. *2010/2011 CSI Computer Crime and Security Survey*. New York: Computer Security Institute.

Salmon, Paul., and N. Stanton. 2008. *Distributed Situation Awareness: Advances in Theory, Measurement and Application to Team Work*. PhD. Brunel University.

Schmittling, Ron. 2010. “Performing a Security Risk Assessment.” *ISACA Journal*, Vol. 1: 1-7.

Shedden, Piya, A. B. Ruighaver, and Atif Ahmad. 2010. "Risk Management Standards - The Perception of ease of use." *Journal Of Information System Security* 6, no. 3: 23-41.

Shedden, Piya, Rens Scheepers, Wally Smith, and Atif Ahmad. 2011. "Incorporating a knowledge perspective into security risk assessments." *VINE: The Journal of Information & Knowledge Management Systems* 41, no. 2: 152.

Siponen, M. 2006. "Information Security Standards Focus on the Existence of Process, not Its Content." *Communications of the ACM* 49, no. 8: 97-100.

Siponen, Mikko and Robert Willison. 2009. "Information security management standards: Problems and solutions." *Information & Management* 46, 267-270.

Treverton, Gregory F., and C. Bryan Gabbard. 2008. "Assessing the Tradecraft of Intelligence Analysis." RAND National Security Research Division Technical Report.

Treverton, Gregory F., Seth G. Jones, Steven Boraz, Philip Lipscy. 2006. "Toward a Theory of Intelligence." RAND National Security Research Division Workshop Report (Conference Proceedings).

US Government. 2009. *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis*. Washington, D.C.: US Central Intelligence Agency, Center for the Study of Intelligence.

Utin, Daniil M., Mikhail A. Utin, and Jane Utin. 2008. "General Misconceptions about Information Security Lead to an Insecure World." *Information Security Journal: A Global Perspective* 17, no. 4: 164-169.

von Grebmer, Andreas. 2007. *Information and IT Risk Management in a Nutshell: A Pragmatic Approach to Information Security*. Norderstedt, Germany: Books on Demand.

Whitman, Michael E., and Herbert J. Mattord. 2004. *Management of information security.* Boston, Mass. Thomson Course Technology.

Yin, Robert K. 2009. *Case Study Research: Design and Methods.* Thousand Oaks, California: SAGE.

Young, Randall, and John Windsor. 2010. "Empirical Evaluation of Information Security Planning and Integration." *Communications of AIS* 2010, no. 26: 245-266.

COPYRIGHT