Received 5 September 2018
Revised 9 November 2018
21 December 2018
Accepted 8 January 2019

Revisiting information security risk management challenges: a practice perspective

Erik Bergström
School of Informatics, University of Skövde, Skövde, Sweden, and
Martin Lundgren and Åsa Ericson
Department of Computer Science, Information Systems, Luleå University of Technology, Luleå, Sweden

Abstract

Purpose – The study aims to revisit six previously defined challenges in information security risk management to provide insights into new challenges based on current practices.

Design/methodology/approach – The study is based on an empirical study consisting of in-depth interviews with representatives from public sector organisations. The data were analysed by applying a practice-based view, i.e. the lens of knowing (or knowings). The results were validated by an expert panel.

Findings – Managerial and organisational concerns that go beyond a technical perspective have been found, which affect the ongoing social build-up of knowledge in everyday information security work.

Research limitations/implications – The study has delimitation as it consists of data from four public sector organisations, i.e. statistical analyses have not been in focus, while implying a better understanding of what and why certain actions are practised in their security work.

Practical implications – The new challenges that have been identified offer a refined set of actionable advice to practitioners, which, for example, can support cost-efficient decisions and avoid unnecessary security trade-offs.

Originality/value – Information security is increasingly relevant for organisations, yet little is still known about how related risks are handled in practice. Recent studies have indicated a gap between the espoused and the actual actions. Insights from actual, situated enactment of practice can advise on process adaption and suggest more fit approaches.

Keywords Asset valuation, Information security, Practice theory, Risk management

Paper type Research paper

Introduction

Information Security Risk Management (ISRM) has been defined as a continuous process to identify and mitigate risks towards an organisation's critical information assets. More than a decade ago, Kotulic and Clark (2004) highlighted the importance of empirical studies in ISRM. Since then, little is still known about how organisations protect themselves in practice (Baskerville *et al.*, 2018). The lack of empirical understanding makes it difficult to draw insights on how organisations actually conduct ISRM, what challenges they are confronted with in their tasks, and the nature of knowledge required to mitigate them. Lately, researchers have further pointed out a need for practice-based research within the information security domain. Niemimaa (2016) and Alaskar *et al.* (2015), for example, noted that most empirical research focuses on intention rather than actual behaviour. As a result, they recommend that future studies should be conducted on actual practice to illustrate

Information & Computer Security
Vol. 27 No. 3, 2019
pp. 358-372

2056-4961
DOI 10.1108/ICS-09-2018-0106

further how management processes do not always follow the espoused pattern in standards. Similarly, Shedden *et al.* (2010) stressed in their study the importance of a practice-based perspective to ISRM to explore its effectiveness within organisations. Likewise, Alshaikh *et al.* (2018) have demonstrated an applied practice-based lens to closer align security training with the organisational context, while Öbrand *et al.* (2012) grounded their study on a practice-based approach to understand better how risk management activities emerged over time. Thus, to the best of our knowledge, a few studies have shown the potential of a practice-based lens.

A consequence when disregarding practice may lead to overvaluing the formal approaches while undervaluing situated enacted activities, i.e. how practice adapts its processes to real situations (Jarzabkowski *et al.*, 2016). One example of this can be seen in the growing misconception that compliance with formal processes is equivalent with good security (Kwon and Johnson, 2013; Webb *et al.*, 2016). Not only does this leave many organisations more concerned with accommodating rather than developing and adapting security practices tailored to their unique context (Kwon and Johnson, 2013; Webb *et al.*, 2016), it has also been shown that strictly following formal practices will be "de-skilling to practitioners because creativity and reflexivity is stifled" (Njenga and Brown, 2012, p. 594). In other words, practice is what gives actual, contextual meaning and locally produced knowledge to formal approaches, and should be studied as it has proven to provide valuable insight to ISRM for practitioners and researchers alike.

This paper aims to provide insights into new challenges that are grounded in organisational management of information security processes. The study revisits six previously defined challenges from Fenz *et al.* (2014) and, by doing so, our effort is to progress further research on practice-based theory in the ISRM field by translating challenges to reflective actions, called knowings.

This paper is organised as follows; the next section discusses current ISRM processes and associated challenges, while the section after that presents the study approach. The following section presents and discusses the empirical findings. The next section accounts for the results, i.e. proposes a number of relevant insights for practice, and the final section concludes the study.

Challenges in the current Information Security Risk Management processes

Information security risk management processes

Over the past decades, the development of various ISRM processes has gained attention in the literature (ISO/IEC 27005, 2013; Bowen *et al.*, 2006; NIST SP 800-30 2012). To be applicable in different contexts, such processes are designed to be universal in scope, focusing on "formal, rule-based descriptions of procedures to be followed" (Njenga and Brown, 2012, p. 594). Therefore, risks towards information assets are seen as something that can be controlled if managed rationally and sequentially (Coles-Kemp, 2009; Dhillon and Backhouse, 2001).

Typically, these procedures' descriptions emphasise processes for measuring and identifying valuable assets within the organisation and selecting means of controlling risks towards those assets based on predictions and historical comparisons (Baskerville *et al.*, 2014). Standards such as ISO/IEC 27005 (2013) and NIST SP 800–30 (2012) outline a continuous process to identify assets and existing countermeasures, assess risks and their likelihood to mitigate or accept those risks (ISO/IEC 27005, 2013; NIST SP 800-30, 2012). Furthermore, researchers such as Straub and Welke (1998) and Spears and Barki (2010), have similarly outlined ISRM as containing activities for identifying and prioritising information assets and security risks to implement and monitor countermeasures.

Evaluation of additional ISRM processes has also shown that there are only minor differences in their description (Fenz *et al.*, 2014). While varying in specific steps or depth, the process descriptions typically include activities for identifying and valuing assets, predicting risks and implementing adequate countermeasures (ISO/IEC 27005, 2013; Shedden *et al.*, 2010; Whitman and Mattord, 2014; Visintine, 2003; Baskerville *et al.*, 2014).

Six challenges in Information Security Risk Management

Fenz *et al.* (2014, pp. 419-422) find it achievable to theorise on the main challenges for organisations. Therefore, they propose, six current and fundamental challenges that still effect how risk managers come up with sound results. Starting from these six challenges as a frame of reference, additional input from the literature has here been used to refine each challenge's description. The refined challenges can thus be presented as follows:

Asset and countermeasure inventory. The challenge relates to the problems of identifying what would be a valuable asset to protect and what potential countermeasures could be used to protect the asset. The challenge relates to, e.g. how to identify information capital (Bunker, 2012; Ku *et al.*, 2009), especially considering that information is everywhere and can take any shape (Saxby, 2008). Additionally, most ISRM processes lack a reliable asset inventory approach (Vose, 2008) adding complexity to the challenge.

Assigning asset values. The challenge relates to the actual assignment of a value to an asset. This includes, e.g. the basics of such estimations (Aksentijevic *et al.*, 2011; Al-Fedaghi, 2008), a lack of motivation for valuation among colleagues (Hayes, 2008) and the subjective judgment (Glynn, 2011; Kaarst-Brown and Thompson, 2015) associated with it. Furthermore, the development of classifications (Baškarada, 2009) is based on too generic standards (Bayuk, 2010), which can be troublesome for organisations. Also, deciding the granularity of the information (Blyth and Kovacich, 2006) and getting it performed consistently in the organisation (Eloff *et al.*, 1996) is difficult, especially considering that technology cannot solve the problem (Everett, 2011).

Failed predictions of risk. The challenge is described in relation to an attacker's interest in the organisation's assets. That interest is hard to predict as it changes over time. Prevention of predicted threats is inherent in the actual paradigm of ISRM (Baskerville *et al.*, 2014). However, not all risks are predictable, measurable and persistent (Taylor, 2015); some are more unpredictable and better suited to interpretive approaches (Spagnoletti and Resca, 2008).

The overconfidence effect. This challenge relates to managerial issues not typically addressed in standards and frameworks (Fenz *et al.*, 2014). Challenges include managerial styles that are often grounded in being far too optimistic (Taylor, 2015; Rhee *et al.*, 2012), the authority of information security leaders (Collette, 2006; Taylor, 2015) and a lack of standards for particular sectors (Janczewski and Xinli Shi, 2002).

Knowledge sharing. This challenge relates to the necessity of sharing information in and between organisations. Awareness of this challenge can be useful in risk prediction to assess better how information and knowledge assets are put at risk (Padyab *et al.*, 2014). Knowledge sharing is important to sustain the operational complexity in risk prediction and rests both individually and collectively within people (Shedden *et al.*, 2011).

Risk vs cost trade-offs. This challenge relates to being cost-effective in balancing costs of countermeasures and the expected loss of an asset. The challenge identifies the lack of cost estimation techniques related to risk management activities as one of the main weaknesses of current risk management processes (Sadok and Spagnoletti, 2011; Lawrence *et al.*, 2003).

Study approach

Data collection

To capture reasoning in practice, a qualitative research approach was designed. To gain an understanding of organisations ISRM processes, rich insights could be based on sampling from a few respondents possessing expertise in the chosen area (Kvale, 1996; Patton, 2014). Therefore, statistical generalisations were not sought after, but instead, saturation of the chosen topics, i.e. patterns in the answers can be identified and themes reoccur (Mason, 2002).

Considering the difficulty to obtain field data on how ISRM processes are enacted in practice (Baskerville *et al.*, 2018; Kotulic and Clark, 2004), Swedish public sector organisations were chosen. The reasoning behind this was twofold. Firstly, owing to the principle of public access to official records, internal policies are generally more accessible. Secondly, the Swedish public sector is required to work systematically with ISRM; however, there is no nationally enforced standard. Thus, the public sector has adopted different ISRM approaches in practice.

The organisations included in this study were selected on the basis of their expertise and that they had well-documented policies and implemented procedures. A study on Swedish ISRM practices revealed, however, that despite being a requirement, only 60 per cent of Swedish Government agencies have an established activity for risk management, and only 43 per cent have one for asset valuation (Swedish Civil Contingencies Agency, 2014). Drawing on the result of a large survey in governmental Sweden (Bergström *et al.*, 2018), four public sector organisations were chosen for this study. Each organisation represented a different sector providing functions critical to society, and demonstrated particularly mature ISRM processes. The organisations provided their internal policy documents for analysis, which added secondary data to the study. The key responsible ISRM roles within the respective organisation were identified in parallel with the review of the internal policies and were interviewed. In three of the four organisations, the selected interviewees were also the writers of their respective internal policy. An overview of the organisations and interviewees is presented in Table I.

An interview guide was developed based on the six refined challenges. Thirty open-ended questions (Bryman and Bell, 2011) were formulated as a basis for the interviews, targeting ISRM activities and practices. The questions were open-ended to avoid imposing our perceptions on their answers. Altogether, the interviews and the internal policies gave rich insights into motivations and reasoning among the respondents.

Each interview lasted between 50 and 90 min and was recorded. The recordings were divided among the authors for transcription in its entirety and double-checked by each other, resulting in 52 pages of transcriptions.

Data analysis

The practice lens of organisational creation of meaning, in short, "knowing" or "knowings", was applied for finding the unit of analysis. Knowing is described by Orlikowski (2002, p. 249) as follows:

ID	Sector	No. of employees	Role(s)
Alpha	Health and social affairs	~1, 200	Security Specialist
Beta	Environment and energy	~650	Security Architect
Gamma	Enterprise and innovation	~2, 000	Information Security Coordinator, and IT-Architect
Delta	Public sector coordination	~230	Director of Preparedness and Response

Table I.
Background details on the organisations and interviewees

> Purposive and reflexive, continually and routinely monitoring the ongoing flow of action–their own and that of others—and the social and physical contexts in which their activities are constituted.

The important perspective here is to apply knowing as a verb indicating action, doing and practice. Thus, the transcribed answers were first categorised, using concept-driven coding (Spencer and Ritchie, 2002). The categorised material was then discussed and merged into a new document and thematised into themes of knowing through the practice-based lens, emphasising enacted activities that got "their work done".

Validation

In ISRM research, there is a general lack of validation, and there are various approaches on how to perform it (Fenz and Ekelhart, 2011). Silverman (2015) recommends qualitative research approaches to take the results "back to the people" to see if they conform to their own experiences. Similarly, Fenz and Ekelhart (2011) suggest that expert panels are a good approach for validating ISRM results as it is one of the few ways that accounts for various real-world parameters.

Hence, to validate the knowings and practices that met the refined challenges in practice, opinions were sought from a broader set of information security managers. An expert panel consisting of 16 senior information security managers from public sector organisations was organised. None of the participants in the expert panel came from the four organisations targeted in this study. The expert panel consisted of nine chief information security officers, two chief technology officers, and the remaining five had other various information security management roles.

The expert panel was held as an hour-long session, where the authors presented how the challenges had been met in practice, followed by discussions. The session was recorded and transcribed.

Empirical results

One of the common pitfalls in practice-based research is taking the existence of isolated entities for granted (Feldman and Orlikowski, 2011). To address this, the empirical result was divided into its respective challenge and referenced to the organisation making a claim.

Asset and countermeasure inventory

The investigated organisations acknowledge the difficulty in identifying information assets with high granularity. They have instead moved towards identifying the systems in which the information resides in, to abstract the level of detail and by having a direct relation between asset values and countermeasures. This approach rests on the belief that different information types may exist within the same system, and that it makes sense for them to value the whole system based on the most sensitive information present in the system. A consequence is that they over-protect some information, but the difficulty of implementing a variety of countermeasures matching the different valuations on the same system is a greater challenge and considered a less effective use of resources.

Alpha and Beta both emphasised that they perform an in-depth initial identification of all infrastructure systems present in their respective organisations, and are valuing the infrastructure with regard to present or needed countermeasures. They explained that this approach makes the system identification, and hence the subsequent valuation easier. Because all information flows and connections in entangled systems do not need to be

investigated as thoroughly, since the information flows will inherently be protected if the infrastructure is protected. Alpha justified this as follows:

> Instead of digging down in each individual [information] flow, every row, [. . .] I mean if you do not have matching countermeasure levels later [. . .] [which is] a common approach to valuation, what's the meaning by noticing the difference [in value] between different rows?

Another motivation for the system identification approach was given by Gamma who believed that it can be seen as positive when some information is over-valued and henceforth over-protected in a system as it is considered too hard to capture all changes to the asset value over time in its life-cycle.

An additional insight also came from Gamma that pointed out that the organisation does not necessarily have to invest in identifying and valuing all information, but rather do it on-demand and to start where it gives the most "bang for the buck". For example, if there are changing risks to a system, it could, as clarified by Gamma, trigger a new valuation.

The investigated organisations can be said to have a viewpoint where the valuation of the identified information is not separated from countermeasures, but rather that countermeasures are a consequence of the valuation. The organisations have either established a direct link in their internal policies between information value and specific countermeasures, or they have a clear understanding of what certain information values would require regarding countermeasures. Beta, for example, expressed this as follows: "and then, from the valuations, we knew what kind of information [we possessed], and then we also knew what types of protection we wanted to apply". Furthermore, both Beta and Delta highlighted that it is important also to perform an inventory of laws and regulations that affect the organisation as they can be used as a motivation for defining minimum requirements on countermeasures.

It was also pointed out by the investigated organisations that one should be aware that the implemented countermeasures reflect a snapshot in time of the system and that countermeasures effectivity and information values change over time. Beta pointed out that either they have to do new valuations regularly over time or it has to be incident-driven so that systems that are often affected by incidents have to be revalued.

Assigning asset values

The organisations have all spent considerable effort in establishing the groups performing the valuation, finding ways to motivate the employees, and defining the role of the valuation in the ISRM process.

Determining the value of information assets is described in the literature as difficult and problematic because of the subjective judgment that has to be made. The investigated organisations suggested that a concrete way of reducing this subjectivity is to have a clearer link between information types and countermeasures as described earlier, in which specific countermeasures match the consequence of a valuation. The benefit of using predefined values for certain information types, which also increase consistency, throughout the organisation, align with the suggested approach.

Similar to the findings in the challenge of inventory of assets and countermeasures, the organisations that chose a system valuation approach allows a larger group with diverse skills and experiences to participate and highlight the information in a system, and its use from several perspectives. Such a group-based workshop approach with open discussions has been adopted by the investigated organisations. Gamma adds that the workshops are trying to consider the information life-cycle to capture all stakeholders. The group-based workshops invite, for example, lawyers in the valuation process at both Beta and Gamma.

Beta invites many different competencies, or in their terms, "the right people" to the valuations, to get an as unbiased view as possible of the information assets in question, including those finally responsible for implementing the countermeasures. Ultimately, whom to involve in the workshop depends on what system is being valued and which stakeholders it addresses. Gamma also states that it is important to understand that group composition is something that will take shape over time and that one cannot specify the participants from the very beginning.

The respondents expressed that it is difficult to motivate employees to perform the valuation. Alpha has tackled this challenge by following up the results of the valuation and by making the results visible throughout the entire ISRM process. In Alphas words, the valuation

> Is important, and considering the time it takes, it should result in something more than just putting a label on the information. Otherwise, everyone will start wondering; 'Ok, this information was so important, what happens now? Why don't they care about it half a year later?' So it is very important that it is actually followed-up [. . .] so that the organisation can confirm throughout the [ISRM] process.

An important additional aspect is to ensure that there is a clear output of the valuation that goes into the risk prediction, not only the numeric value itself but also contextual information about usage and users to help motivate countermeasures.

Failed predictions of risk

Contrary to suggestions from the literature on ISRM processes, none of the organisations conducted risk prediction in the suggested way. Risk prediction was seen as a complex and highly time-consuming activity. Because of this, it became mostly an activity to rank pre-determined countermeasures to be implemented on the basis of a fixed list of risks, and not applied as an activity to uniquely choose countermeasures based on risk predictions.

However, both Alpha and Beta used to conduct risk prediction but soon found that the same or similar risks appeared each time. Consequently, Beta stopped conducting risk predictions on smaller systems unless there was a reason to believe that a particular system was targeted by unexpected risks. Instead, Beta abstracted their component for analysis to entire infrastructures. Beta argued that "we have a pretty good understanding of what assets are important within the infrastructure, so it makes sense to focus the risk prediction on the infrastructure". Furthermore, Alpha does not use risk prediction to decide on final countermeasures. Instead, they have correlated particular asset values with particular countermeasures. Nevertheless, risk prediction still plays a part in Alpha's work, but merely as a filter to determine in what order to implement the countermeasures. Previously, Alpha used to have an algorithm to help calculate and prioritise what countermeasures to implement. However, as no one in the organisation used it, the responsibility of determining the order of countermeasures to implement came to rest with the system owner. Interestingly, Beta and Alpha recognise that their current approach might not provide as much detail as otherwise characterised by traditional approaches in risk prediction. Alpha states that they will inevitably "miss maybe 5 per cent of risks that are never found, and the only way to find them is to make unique risk predictions", yet they conclude, "[. . .] our way of doing it still covers most of all risks, and it provides much better use of resources".

Delta and Alpha argue that software tools could only theoretically help to conduct risk prediction, but would be practically infeasible. They build their argument on the notion that a continuous stream of risk predictions is not reasonable considering the required implementation and monitoring of countermeasures. Alpha describes that

> Even though I could wish that we had risk prediction software [. . .] no, that is not for us. When we work with this in practice, after an asset has been valued, several countermeasures are already mandated, something that can take 6-18 months to implement.

Beta notes that the skills for how to manage risk are not easily shared, something they have spent much time trying to perfect. The only successful approach, according to Beta, is to simply exercise risk management over a long period to reach organisational fit.

The overconfidence effect

To overcome some of the challenges posed by the overconfidence effect, the organisations had, to avoid ambiguity, developed a clear ISRM process accompanied by tailored guidelines and expectations for daily work. Additionally, top managers were assigned responsibilities for final decisions on organisation-wide countermeasures.

Alpha, for example, use established formats describing the relations between asset values and specific countermeasures. This documentation has, in turn, removed some of the ambiguous decision-making in finding suitable countermeasures. Consequently, top managers decide the final risk acceptance, and will also be responsible for determining additional countermeasures that go outside what has been established. This has made the process more transparent to the entire organisation. Similarly, for Gamma, this has also worked as a motivator in sanctioning additional economic support from top managers.

In an effort to cultivate the established ISRM process, Alpha and Beta have, as they describe, dedicated plenty of resources trying to educate employees about its activities through workshops and tailored guidelines. Alpha expresses that having a clear, detailed outlined ISRM process is key to success as "it gives a clear benefit for the organisation, and the organisation itself experience the [ISRM] process as something that adds value and is of use for them". Alpha even indicates that they do not want an extensive "ISRM manual" but rather target-oriented instructions for all employees. Gamma takes it one step further and uses an approach that can be described as need-to-know, where only the closest ones will learn about, for example, how to perform the valuation. Beta similarly develops their guidelines by tailoring it to the targeted employees by elaborating questions such as "How would these requirements be met and understood by the targeted audience?" and "How can we change it to make the message clearer?".

An organisation-wide understanding of the ISRM activities affected Alphas and Betas' attitude towards information security. Rather than seeing ISRM as a hindrance or something only necessary to abide by laws and regulations, ISRM was believed to have ethical or moral consequences. In Betas case, for example, compliance was motivated because there could be dangerous consequences in the real world if systems were not adequately protected. Similarly, Alpha had a culture of *quis custodiet ipsos custodes* (who will guard the guardian). For example, during system development, intended system owners will critically review the predefined requirements in a series of dialogues with the developers. Because the system will ultimately be assessed by a champion to assure its countermeasures, developers and future owners have realised that any shortcuts will inevitably be more costly in the end for both parties.

Knowledge sharing

An important aspect of tackling the challenge of knowledge sharing is how to accomplish a coherent ISRM process in practice. All the organisations stressed the importance of including a champion with key skills in all the activities of the ISRM process, making these champions the glue that makes the processes coherent. The investigated organisations saw different champions. For example, Alpha saw a security specialist as a champion, while

Gamma saw an IT architect. Having a champion contribute to reducing problems with different views on asset valuations, and offer an inherent possibility of monitoring the whole ISRM process. Beyond a champion, it was also stressed that the organisational side with its knowledge of how and by whom certain information is used, together with the IT department with its technical know-how, are represented and participate throughout the whole ISRM process. This knowledge does not need to be in-house, as shown by both Delta and Gamma. Instead, they collaborate closely with other similar organisations within their respective sectors, to borrow and share competence when needed, such as technical know-how for a particular system.

Beta expressed that they have dialogues that are not part of the formal ISRM process, but that add insight. For example, when systems are being procured or developed, an effort to capture requirements, or perform preliminary valuations are made. These informal dialogues are initiated either by the champions, from the procurement or development side. It is viewed by Beta as a sign of a mature ISRM process because the champions do not have knowledge of everything in progress within the organisation and point out that it also limits the risk of having the ISRM process rely solely on a particular champion.

Another knowledge-sharing enabler described was that the organisations chose to homogenise their language internally, i.e. a shared vocabulary, to avoid misunderstandings. An example of this is how information types and risk activities were referred to by the respective organisations, both in the interviews and in their written policies. Delta described it as follows:

> We have some kind of definition [of key concepts] that we cannot get crystal clear, there are always grey areas, but as far as we can, we try to define what we mean by different concepts.

Risk vs cost trade-offs

The investigated organisations see countermeasures as a result of the valuation. Therefore, the discussion about cost does not derive from risk but rather the asset valuation. Because of this, the discussion focused on the cost associated with countermeasures, and not risks.

Although the relation between asset value and countermeasures were perceived as obvious, the cost trade-off in practice was not. This was shown through various examples, as for instance at Gamma, they perceived their policy as running short with respect to cost consequence, or as they described it:

> The policy for assigning asset values are clear and easy to follow, [. . .] but I think there is still something missing, some parameter for reaching a decision on countermeasures in terms of time and money.

Gamma further described that it is common that this ambiguity, in the end, leads to more time spent on searching for less expensive countermeasures. Beta explained that instead of looking for less expensive countermeasure alternatives, they reconsider the asset value altogether when facing the challenge of cost trade-off. Alpha clarified that they already deal with this challenge during the valuation by including an economic perspective by calculating the estimated economic consequences of a loss. The resulting estimated cost helps justify expensive countermeasures for top managers.

Alpha, Beta and Delta express that this challenge can be met by establishing national requirements, by relating certain information types with particular countermeasures. Such requirements would decrease the uncertainty, as explained by Beta, "by stating that 'these countermeasures are standardised in Sweden,' because then you can say 'this information

shall be protected using these countermeasures,' so that everybody knows what is expected".

Finally, the organisations highlighted the cost of the ISRM process itself. To achieve a coherent process that matures over time, both time and money have to be allocated.

Insights for practice

By analysing the empirical result, a set of knowings can be formulated that describe the enacted practice of how the challenges are reflected upon and how the ongoing collective flow of actions and reasoning create a rationale for the work. The connection between challenges, how they are met in practice and how knowings are constituted are outlined in Table II below.

These identified challenges and suggested knowings have theoretical and practical implications, as follows:

Knowing how to be "good enough": because security is not following a recipe of fortification, but are efforts to apply its principles in the organisations daily work. The organisations described countermeasures as "a snapshot" whilst also acknowledging that they change over time. Recognising that there was no recipe to follow, reaching a "good enough" mentality would, therefore, ensure security processes to be refined and adapted. Not recognising this could be a reason why organisations often perceive security as an obstacle rather than a support. For example, valuing systems instead of information results in less time spent on identification and more time spent on assigning asset values. According to the expert panel in the validation, this approach also resonates better with services where control over the security controls are outsourced. For example, cloud services were mentioned as such services where the security controls many times are pre-determined by the service provider. Directly associating valuation with countermeasures becomes a natural effect of using such services. Furthermore, directly associating valuation with countermeasures removes some of the ambiguity in the asset valuation. Therefore, systems or entire infrastructures were mainly targeted for identification. Finally, the practice of making an initial in-depth identification of infrastructure was recognised in the discussion, but it was pointed out that it could lead to overprotecting parts of the infrastructure, which, in turn, cost more money for the organisation.

Knowing how to hurry slowly: because ISRM implementation costs time and money. It takes time to find which stakeholders to include and to what extent, what competence is required and the time it takes to put together a team. This can be seen as overwhelming if the work does not progress at a pace that is aligned with the rest of the organisation. One such example was described by an expert during the validation, where their organisation had suffered from an information overflow when attempting to valuing all information at the beginning of their ISRM process. Whilst it is tempting to assume managers will make correct and rational decisions at the early beginning of the ISRM process, such overconfidence could pressure managers to make hasty decisions that could be more costly in the long run. Similarly, investing in countermeasures can give an instant result, but lower security over time if compared with investing in an organisationally fit ISRM implementation. Instead, the experts agreed that it might be better to start out slowly with a few critical systems and learn from this process before proceeding with other systems in the organisation. Identify and assign champions could, however, help balance the implementation by both double check the ISRM progress and the overall organisational fit of the ISRM process.

Knowing there is no silver bullet: because it is often suggested to use software tools to help assess risks, countermeasures and assets, the interviewees said that such tools seldom take

Challenges from Fenz *et al.* (2014)	Challenges as met in practice	Knowings constituted in the practice
Asset and countermeasure inventory	Raise the abstraction level by identifying the most sensitive information types in systems	Knowing how to be "good enough"
	An initial in-depth identification of all infrastructure makes valuation easier	Knowing how to be "good enough"
	Make valuation on-demand where it gives most "bang for the buck"	Knowing there is no silver bullet
	Be aware that implemented countermeasures reflect a snapshot in time	Knowing how to be "good enough"
Assigning asset values	Use predefined valuations for certain information types to create a direct relation between valuation and countermeasures	Knowing how to be "good enough"
	Accepting that a coherent ISRM implementation cost time and money	Knowing how to hurry slowly
	Use workshops with diverse skills and experiences when valuing	Knowing how to hurry slowly
	Follow up the valuation throughout the ISRM process to support and motivate employees	Knowing the bigger picture
Failed predictions of risk	Risk prediction reduced to rank pre-determined countermeasures based on a fixed list of risks	Knowing how to be "good enough"
	Being completely updated on real-world risks is practically infeasible	Knowing there is no silver bullet
	Favour simplicity over complexity and accept not all risks can be found	Knowing how to be "good enough"
The overconfidence effect	Clear ISRM process with tailored guidelines and training	Knowing the bigger picture
	Top managers make final decisions of countermeasures	Knowing the bigger picture
	Top managers own risk acceptances	Knowing the bigger picture
	Ethical and moral consequences motivate the ISRM process more than laws and regulations	Knowing there is no silver bullet
Knowledge sharing	Identify a champion with key ISRM skills	Knowing how to hurry slowly
	Champions are the glue that makes the ISRM process coherent	Knowing the bigger picture
	Informal dialogues are encouraged to reach common expectations about the ISRM activities	Knowing the bigger picture
	Homogenise the internal language to avoid misunderstandings	Knowing the bigger picture
Risk vs cost trade-offs	Cost associated more with countermeasures than risks as the trade-off is made between countermeasures and the economic consequences of information loss	Knowing how to be "good enough"

Table II.
An overview of the empirical results highlighting ISRM challenges as found in literature, how they are met in practice, and constituted as knowings

social or organisational aspects into account. For example, this was shown where organisations had moved beyond using or even wanting to use, such tools because it was not feasible in daily work, e.g. it did not give a return on investment, i.e. "bang for the buck". Staying updated about, e.g. all real-world risks were not found to be the main issue, but rather the time required to act upon them. Similarly, being completely updated on real-world risks does little to socially motivate actions. Instead, risk is too subjective to be beneficial by

simply being updated, and requires practical experience, or knowings, which can only be obtained over time. It was, for example, shown that requirements such as laws and regulations, did not motivate the ISRM process, but intrinsic values did. The expert panel confirmed this and acknowledged the importance of emphasising ethical and moral consequences. However, they had a lengthy discussion on the difficulty in recognising such intrinsic values for different groups. For instance, when motivating economists, economic consequences could be more beneficial to use than ethical and moral consequences.

Knowing the bigger picture: because the various activities within ISRM should be enacted as a holistic entity that is aligned with the organisation's goal. Recognising that the ISRM process is more than the sum of its activities was seen as mature praxis. One should not see each activity within the process as producers and consumers of input and output but as decisions that are shaped and reshaped. In other words, it means realising that organisational alignment is the result of joint effort throughout the entire process, with active feedback from champions, informal dialogues, workshops and training activities to reach unanimous ideas and expectations. Several members of the expert panel were champions in their respective organisations and gave additional input on how to achieve this in practice. For example, at the start of a valuation or risk prediction, they gave an introduction regarding the aim, objective and expectations of the task at hand to raise the participants' level of understanding. Activities such as these are seen as a dynamic learning process that is kept alive. Thereby, the activities make sense for the organisation. One example of this is that it is difficult to know exactly whom to include, something that will become clearer over time as the ISRM process evolves, which was also acknowledged by the expert panel.

Conclusions

This paper aimed to provide insights into new challenges that are grounded in organisational management of information security processes. The study revisited six previously defined challenges (Fenz *et al.*, 2014) and, by doing so, the effort was to progress further research on practice-based theory by translating challenges to reflective actions, called knowings. These have been formulated as knowing to be "good enough", knowing to "hurry slowly", knowing "there is no silver bullet" and knowing the "bigger picture". In this paper, it was thus illustrated how a practice-based lens could contribute to further insights into how context could shape practice. That is to say, content within management processes is not created by the espoused descriptions found in standard approaches but in practice formed by employees' ambition, intent and experiences. This was observed empirically, and validated by an expert panel, in which the relationship between activities as well as their content evolved as a result of what "made sense" for the practitioners. Hence, one implication for research is that much can be learned by focusing on what people do in practice, as opposed to what they should do. The identified knowings offer a base for further research in this respect.

Studies on practice, as shown here, may have the potential to be realised by practitioners and managers who are struggling with ISRM implementation (Shedden *et al.*, 2010). This paper has described examples of how a practice-based lens can provide actionable advice. It is stressed in formal standards that ISRM processes should align with organisational objectives, but there is little advice on how to do that in practice. One implication for practitioners that can be seen here is that the examples emphasise that everyone involved in the actions contribute to a shared understanding that benefits organisations. The investigated organisations showed various reflective actions to overcome such challenges, for instance, by using informal dialogues to reach common expectations about the ISRM activities or by homogenising the internal language to avoid misunderstandings, as shown in knowing "the bigger picture". Another implication for practice is that allocating resources

to identify whom to include in the process would probably benefit the subsequent work and provide for a less biased result. This was observed in practice by the use of champions, and workshops where it was emphasised to "hurry slowly". Finally, a third implication for practice is that "good enough" combined with continuous reflections could be a doable approach to deal with the fact that risks and thus also the countermeasures change over time.

References

Aksentijevic, S., Tijan, E. and Agatic, A. (2011), "Information security as utilization tool of enterprise information capital", *Proceedings of the 34th International Convention MIPRO*, 23-27 May, pp. 1391-1395.

Al-Fedaghi, S. (2008), "On information lifecycle management", *Proceedings from the 2008 Asia-Pacific Services Computing Conference*, 9-12, December, pp. 335-342.

Alaskar, M., Vodanovich, S. and Shen, K.N. (2015), "Evolvement of information security research on employees' behavior: a systematic review and future direction", *Proceedings of the 48th HI International Conference on System Sciences*, pp. 4241-4250.

Alshaikh, M., Maynard, S.B., Ahmad, A. and Chang, S. (2018), "An exploratory study of current information security training and awareness practices in organizations", *Proceedings of the 51st HI International Conference on System Sciences*, pp. 5085-5094.

Baškarada, S. (2009), "Analysis of data", Information Quality Management Capability Maturity Model, Vieweg+Teubner, pp. 139-221.

Baskerville, R., Rowe, F. and Wolff, F.-C. (2018), "Integration of information systems and cybersecurity countermeasures: an exposure to risk perspective", *ACM Sigmis Database: The Database for Advances in Information Systems*, Vol. 49 No. 1, pp. 33-52.

Baskerville, R., Spagnoletti, P. and Kim, J. (2014), "Incident-centered information security: managing a strategic balance between prevention and response", *Information and Management*, Vol. 51 No. 1, pp. 138-151.

Bayuk, J. (2010), "The utility of security standards", paper presented at 2010 IEEE International Carnahan Conference on Security Technology (ICCST), 5-8 October.

Bergström, E., Anteryd, F. and Åhlfeldt, R.-M. (2018), "Information classification policies: an exploratory investigation", in Dhillon, G. and Samonas, S. (Eds), *Proceedings of the Annual Information Institute Conference*, *Las Vegas, NV*, 26-28 March 2018, pp. 26-28.

Blyth, A. and Kovacich, G.L. (2006), "IA and software", *Information Assurance*, Springer London, pp. 191-212.

Bowen, P., Hash, J. and Wilson, M. (2006), *Information Security Handbook: A Guide for Managers*, National Institute of Standards and Technology, Gaithersburg, MD.

Bryman, A. and Bell, E. (2011), *Business Research Methods*, 3rd ed., Oxford University Press, USA.

Bunker, G. (2012), "Technology is not enough: taking a holistic view for information assurance", *Information Security Technical Report*, Vol. 17 Nos 1/2, pp. 19-25.

Coles-Kemp, L. (2009), "Information security management: an entangled research challenge", *Information Security Technical Report*, Vol. 14 No. 4, pp. 181-185.

Collette, R. (2006), "Overcoming obstacles to data classification [information security]", *Computer Economics Report (International Edition)*, Vol. 28 No. 4, pp. 8-11.

Dhillon, G. and Backhouse, J. (2001), "Current directions in IS security research: towards socio-organizational perspectives", *Information Systems Journal*, Vol. 11 No. 2, pp. 127-153.

Eloff, J.H.P., Holbein, L.R. and Teufel, S. (1996), "Security classification for documents", *Computers and Security*, Vol. 15 No. 1, pp. 55-71.

Everett, C. (2011), "Building solid foundations: the case for data classification", *Computer Fraud and Security*, Vol. 2011 No. 6, pp. 5-8.

Feldman, M.S. and Orlikowski, W.J. (2011), "Theorizing practice and practicing theory", *Organization Science*, Vol. 22 No. 5, pp. 1240-1253.

Fenz, S. and Ekelhart, A. (2011), "Verification, validation, and evaluation in information security risk management", *IEEE Security and Privacy Magazine*, Vol. 9 No. 2, pp. 58-65.

Fenz, S., Heurix, J., Neubauer, T. and Pechstein, F. (2014), "Current challenges in information security risk management", *Information Management and Computer Security*, Vol. 22 No. 5, pp. 410-430.

Glynn, S. (2011), "Getting to grips with data classification", *Database and Network Journal*, Vol. 41 No. 1, pp. 8-9.

Hayes, J. (2008), "Have data will travel - [IT security]", *Engineering and Technology*, Vol. 3 No. 15, pp. 60-61.

ISO/IEC 27005 (2013), "Information technology – security techniques – information security risk management", ISO/IEC.

Janczewski, L. and Xinli Shi, F. (2002), "Development of information security baselines for healthcare information systems in New Zealand", *Computers and Security*, Vol. 21 No. 2, pp. 172-192.

Jarzabkowski, P., Kaplan, S., Seidl, D. and Whittington, R. (2016), "On the risk of studying practices in isolation: linking what, who, and how in strategy research", *Strategic Organization*, Vol. 14 No. 3, pp. 248-259.

Kaarst-Brown, M.L. and Thompson, E.D. (2015), "Cracks in the security foundation: Employee judgments about information sensitivity", *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research, Newport Beach, ACM, CA*, pp. 145-151.

Kotulic, A.G. and Clark, J.G. (2004), "Why there aren't more information security research studies", *Information and Management*, Vol. 41 No. 5, pp. 597-607.

Ku, C.-Y., Chang, Y.-W. and Yen, D.C. (2009), "National information security policy and its implementation: a case study in Taiwan", *Telecommunications Policy*, Vol. 33 No. 7, pp. 371-384.

Kvale, S. (1996), *InterViews: An Introduction to Qualitative Research Interviewing*, SAGE Publications, Thousand Oaks, CA.

Kwon, J. and Johnson, M.E. (2013), "Health-care security strategies for data protection and regulatory compliance", *Journal of Management Information Systems*, Vol. 30 No. 2, pp. 41-66.

Lawrence, A.G., Martin, P.L. and Tashfeen, S. (2003), "A framework for using insurance for cyber-risk management", *Commun. ACM*, Vol. 46 No. 3, pp. 81-85.

Mason, J. (2002), *Qualitative Researching*, 2nd ed., SAGE Publications, London.

Niemimaa, E. (2016), "A practice lens for understanding the organizational and social challenges of information security management", *Pacific Asia Conference on Information Systems*, pp. 58-68.

NIST SP 800-30 (2012), *Guide for Conducting Risk Assessments*, National Institute of Standards and Technology, Gaithersburg, MD.

Njenga, K. and Brown, I. (2012), "Conceptualising improvisation in information systems security", *European Journal of Information Systems*, Vol. 21 No. 6, pp. 592-607.

Öbrand, L., Augustsson, N.P., Holmstrom, J. and Mathiassen, L. (2012), "The emergence of information infrastructure risk management in IT services", *Proceedings of the 45th HI International Conference on System Sciences*, 4-7 January, pp. 4904-4913.

Orlikowski, W.J. (2002), "Knowing in practice: enacting a collective capability in distributed organizing", *Organization Science*, Vol. 13 No. 3, pp. 249-273.

Padyab, A.M., Päivärinta, T. and Harnesk, D. (2014), "Genre-based assessment of information and knowledge security risks", in *Proceedings of the 47th HI International Conference on System Sciences*, 6-9 January, pp. 3442-3451.

Patton, M.Q. (2014), *Qualitative Research and Evaluation Methods: Integrating Theory and Practice*, SAGE Publications, Thousand Oaks, CA.

Rhee, H.-S., Ryu, Y.U. and Kim, C.-T. (2012), "Unrealistic optimism on information security management", *Computers and Security*, Vol. 31 No. 2, pp. 221-232.

Sadok, M. and Spagnoletti, P. (2011), "A business aware information security risk analysis method", in D'Atri, A., Ferrara, M., George, J.F. and Spagnoletti, P. (Eds), *Information Technology and Innovation Trends in Organizations*, Physica-Verlag HD, Heidelberg, pp. 453-460.

Saxby, S. (2008), "News and comment on recent developments from around the world", *Computer Law and Security Review*, Vol. 24 No. 2, pp. 95-110.

Shedden, P., Scheepers, R., Smith, W. and Ahmad, A. (2011), "Incorporating a knowledge perspective into security risk assessments", *VINE Journal of Information and Knowledge Management Systems*, Vol. 41 No. 2, pp. 152-166.

Shedden, P., Smith, W. and Ahmad, A. (2010), "Information security risk assessment: towards a business practice perspective", paper presented at Australian Information Security Management Conference 2010.

Silverman, D. (2015), *Interpreting Qualitative Data*, Sage.

Spagnoletti, P. and Resca, A. (2008), "The duality of information security management: fighting against predictable and unpredictable threats", *Journal of Information System Security*, Vol. 4 No. 3, pp. 46-62.

Spears, J.L. and Barki, H. (2010), "User participation in information systems security risk management", *Mis Quarterly*, Vol. 34 No. 3, pp. 503-522.

Spencer, L. and Ritchie, J. (2002), "Qualitative data analysis for applied policy research", in Huberman, A.M. and Miles, M.B. (Eds), *Analyzing Qualitative Data*, Routledge, Thousand Oaks, CA, pp. 187-208.

Straub, D.W. and Welke, R.J. (1998), "Coping with systems risk: security planning models for management decision making", *Mis Quarterly*, Vol. 22 No. 4, pp. 441-469.

Swedish Civil Contingencies Agency (2014), "En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter [a picture of governmental agencies work with information security 2014 – application of the Swedish civil contingencies agency guidelines]", Swedish Civil Contingencies Agency.

Taylor, R.G. (2015), "Potential problems with information security risk assessments", *Information Security Journal: A Global Perspective*, Vol. 24 Nos 4/6, pp. 177-184.

Visintine, V. (2003), "An introduction to information risk assessment", SANS institute, Vol. 8.

Vose, D. (2008), *Risk Analysis: A Quantitative Guide*, John Wiley and Sons.

Webb, J., Maynard, S.B., Ahmad, A. and Shanks, G. (2016), "Foundations for an intelligence-driven information security risk-management system", *JITTA: Journal of Information Technology Theory and Application*, Vol. 17 No. 3, p. 25.

Whitman, M.E. and Mattord, H.J. (2014), *Principles of Information Security*, 5th ed., Cengage Learning.

Corresponding author
Erik Bergström can be contacted at: erik.bergstrom@his.se