Abstract

This paper is largely based on a state of the art report covering the information security (IS) metrics area produced as part of the Controlled Information Security (COINS) research project funded by the Swedish Civil Contingencies Agency (MSB) and the comprehensive literature review conducted while compiling the report. The report's findings are summarized and some of the key issues discovered in the course of the literature review are reflected upon. Additionally, the paper describes a conceptual systemic scheme/model for the research process, while explaining its relevance to the subject area, that may help with resolution of the outlined issues in future research in the area. The paper is written principally with a management/governance (rather than engineering) perspective in mind.


Introduction

To paraphrase the frequently quoted (and misquoted) expression by Lord Kelvin, unless something can be measured, our knowledge of it is insufficient. The readily understood implication of this in the reality of management is that our ability to manage something is directly dependent on our knowledge of it, and that managing something that cannot be (or is not being) measured is generally difficult to near impossible.

This has become increasingly apparent in the field of information security over the past decade (IATAC, 2009) and measurement is, for instance, an explicit requirement in the ISO/IEC 27001 standard (ISO/IEC, 2005). As a consequence, a considerable number of research initiatives have been emerging and culminating in best practice and regulatory standards, methodologies, frameworks, compilations, tools and technologies, etc, being developed or adapted to cover/support security metrics.
The greatest driver for this development for most organizations is the recently amplified regulatory environment, demanding greater transparency and accountability. However, organizations are also driven by internal factors, such as the needs to better justify and prioritize security investments, ensure good alignment between security and the overall organizational mission, goals, and objectives, and fine-tune effectiveness and efficiency of the security programmes.

For instance, a survey by Frost & Sullivan showed that the degree of interest in security metrics among many companies (sample consisted of over 80) was high and increasing (Ayoub, 2006); while, in a global survey sponsored by ISACA, dependable metrics were perceived to be one of the critical elements of information security (IS) programme success by many security professionals and executives, though, they were also deemed difficult to acquire (O’Bryan, 2006).

The emphasis on governance also entails a need for proper measurement and reporting on all the echelons within the organization, starting at the highest level. Another survey instigated by ISACA showed that organizations that are missing an information security governance project had identified metrics and reporting as the areas in their information security programmes where the lack of quality was most noticeable (Pironti, 2006). The correlation shown in this study underlines the need to recognize that measurement and reporting are connected with management on all organizational levels.

While the above is generally acknowledged by measurement standards, guidance documents, and various independent authors, security professionals still often struggle with bridging the gaps between different organizational levels when it comes to information security measurement and reporting. Overcoming misconceptions, obtaining senior management support, and finding out what to measure and how to meaningfully report it across different administrative levels in the organization as to facilitate strategic decision-making are still hard problems that often remain unresolved (Ayoub, 2006; Payne, 2006; Jaquith, 2007; Kark et al., 2007; ITGI, 2008).

The next section explains the paper's foundation and how it contributes to the field, and clarifies its scope. The Extended Background section establishes some conceptual basis behind IS measurement that may facilitate better understanding of the subject and outlines some of the common challenges associated with it. In the Research Efforts section, some prominent examples of initiatives aimed at addressing those and other challenges of IS measurement are categorically listed and summarized. The Analysis and Synthesis section reflects on the preceding two sections and proposes a systemic way of looking at the problem area. The Conclusion section offers some closing statements and concludes this paper.

**Method and Scope**

This paper is largely based on a state of the art report covering the IS metrics area (Barabanov, 2011), produced as part of the Controlled Information Security (COINS) research project funded by the Swedish Civil Contingencies Agency (MSB) and the
comprehensive literature review conducted while compiling the report. The paper summarizes and reflects on some of the key issues discovered in the course of the said literature review and, in addition, describes a conceptual systemic research process scheme/model (while explaining its relevance to the area) that may help with resolution of those issues in future research.

This paper, same as the report on which it builds on, is intended to not be nation-specific. The implication is, for instance, that national standards or governmental guidelines are generally omitted unless they have received some degree of international recognition. Furthermore, this paper deliberately differentiates between information security management (or governance) and systems/software security engineering metrics, and is written with the former (management) perspective in mind. That is not to say, however, that all technical aspects of the subject area are omitted or deemed irrelevant in this context.

**Extended Background**

This section first outlines some of the underlying theoretical concepts behind security metrics and their place in the overall organizational context, and then briefly examines the common challenges to their successful implementation.

**Underlying Theory and Concepts**

**Definition of "metrics".** A degree of ambiguity exists with regard to the exact definition of the term metric, in the information security community. The said ambiguity partially stems from the fact that many publications do not explicitly identify the context in which the term is used in the term's definition, presupposing that the context is readily understood in view of the nature of the publication. Confusion may then arise when the term is used out of the context that it was originally intended for. A notable case in point is the occurrence of the term security metrics in both IS management and software assurance, even though the two assume substantially dissimilar contexts.

Although the different definitions are subject to some variation, after reviewing a number of sources (ISO/IEC, 2009a; Chew et al., 2008; Jaquith, 2007; Herrmann, 2007; McIntyre et al., 2007) it is possible to arrive at certain common characteristics. Specifically, metrics are considered to be measurement standards that facilitate decision making by quantifying relevant data, where measurement refers to the process by which they are obtained. A distinction between a metric and a measurement can also be drawn, where the latter quantifies only a single dimension of the object of measurement that does not hold value (facilitate decision making) in itself, while the former is derived from two or more of the latter to demonstrate an important correlation that can aid a decision. This can be refined even further, though unnecessary for the purpose of this paper.

It can also be generally accepted is that metrics are multidimensional. They have lateral (administrative functions) and hierarchical (administrative levels) properties, where the lower level metrics may "roll up" into the higher level ones. They differ in the collection, analysis, and reporting frequency and period; where the latter can be dependent on the
security programme's maturity. Metrics can also be leading or lagging indicators, that is, reflect either future or previous security conditions (Jansen, 2009).

A number of different publications recommend that, in order to properly serve their intended purpose, IS metrics should possess certain "ideal" characteristics. Although the specific terminology among the various sources differs, it can be said that "good" metrics are, in general, expected to possess the following qualities (Jelen, 2000; Chapin & Akridge, 2005; Herrmann, 2007; Jaquith, 2007):

- Metrics should measure and communicate things that are relevant in the specific context for which they are intended, and be meaningful (in both the content and the presentation) to the expected target audience.

- The value of metrics should obviously not exceed their cost. Measures should be cheap/easy enough to obtain so that potential inefficiencies of data collection do not pull the resources needed for subsequent stages of measurement or in other parts and functions of the organization.

- The timeliness and frequency of measurement has to be appropriate for the rate of change of the targets of measurement so that the latency of metrics does not defeat their purpose. It should also be possible to track changes over time.

- Good metrics should ideally be objective and quantifiable. This implies that they have to be derived from precise and reliable numeric values (and not qualitative assessments, which have potential for bias), and likewise be expressed by using readily understood and unambiguous units of measure.

- Metrics have to be consistently reproducible by different evaluators under similar circumstances and, therefore, a sufficient level of formality is expected from the defined measurement procedures.

It can also be recognized that most, if not all of the above can be augmented through a high degree of standardization and, wherever possible, automation of the measurement related processes.

**Applications of metrics.** In most general terms, within the scope and context of this paper, security metrics can be considered a part or extension of an organization's information security management system/programme. Thus, it can be said that the applications of security metrics are as extensive as the reach of security management in the organization (and scale over time accordingly). This perspective is adopted in the ISO/IEC 27004 and the NIST SP 800-55 information security measurement standards (ISO/IEC, 2009a; Chew et al., 2008).

When properly designed and implemented, metrics can be used to identify and monitor, evaluate and compare, and communicate and report a variety of security related issues;
facilitating decision making with a degree of objectivity, consistency, and efficiency that would not otherwise be feasible.

Some things lend themselves to measurement better than others (i.e. some information is inherently easier to collect and quantify). Nonetheless, even though relative simplicity combined with high precision are generally considered to be some of the main merits of (good) measures, a strong argument can be made in favour of using statistical methods to simply reduce uncertainty concerning a "less tangible" target rather than to eliminate it completely, when the latter is not practicable, so that educated decisions about it can still be made (Hubbard, 2007).

Security metrics also share a notable relationship with risk management. It can be said that many of the decisions that the security metrics support are in essence risk management decisions, since the ultimate purpose of all security activities is management of security risks. Thus, metrics can supplement specific risk management activities by directly contributing input for analysis as well as an organization's overall capability to deal with the risks it faces by facilitating continual improvements to security. Conversely, in order to properly direct and prioritize the information security measurement efforts in view of the organization's actual business risks, output from the risk assessment activities must be used. This relationship, for instance, is highlighted in the ISO/IEC 27004 standard (ISO/IEC, 2009a).

**Common Practical Problems and Challenges**

**What to measure.** Security managers often tend to report information that does not facilitate strategic (or any) decision making for the senior management. It is, in fact, widely recognized that one of the major issues in IS measurement and reporting has to do with the fact that the reported information is often based on what is easier to measure instead of what is actually meaningful strategically (Hubbard, 2007; Jaquith, 2007; Herrmann, 2007; Kark et al., 2007; ITGI, 2008). To exemplify, a survey by Frost & Sullivan (Ayoub, 2006) showed that number of incidents was still the most common IS measurement reported to non-IT managers, which, when not put into context and correlated to something else, is not actually informative (although, the same survey showed that more organizations are starting to realize the importance of demonstrating correlations and trends, and had or were planning to implement some form of trending data, which indicates a positive dynamic concerning the issue).

**How to measure.** It can be readily recognized that metrics adhering to "ideal" characteristics outlined in the previous section are generally desirable. However, in practice they often fall short of achieving these qualities (Chapin & Akridge, 2005; Jaquith, 2007; Jansen, 2009). Perhaps, the two most notable issues can be summarized as follows:

- Qualitative IS measures are still the norm in many organizations (Jaquith, 2007; Jansen, 2009), which means decisions are often based on subjective information and measurement processes are inefficient.
• Quantitative IS metrics that do get produced are commonly not placed in proper context, and thus not utilized to full potential, or are even simple measurements (e.g. number of incidents) that do not show any correlation at all and are not at all useful for decision making as a result (Ayoub, 2006; Axelrod, 2008).

It is generally important to understand what different measure types can and cannot be used to indicate (Herrmann, 2007; Jaquith, 2007; Axelrod, 2008). For instance, Boolean value styled checklist can be used to demonstrate existence of controls but they cannot effectively convey how they are performing, making decisions concerning the subject of whether they meet performance targets and, if not, how they can be improved, more or less impossible. There are some pitfalls in the use of seemingly more statistically sound types of metrics as well, however. For example, averaging out performance of a number of controls may provide an easily understandable yet still informative measure of the overall posture of some organizational unit, however, it also obscures the outliers (e.g. some controls can be performing below the expected performance target even though the average may be above it; the averaged out metric obscures this kind of information) (Boyer & McQueen, 2007; Jaquith, 2007).

**How to report.** There are three major problems that can be identified in the common current practices of information security reporting. They can be summarized as follows:

• Precise numeric values may be used to represent measures that are obtained by qualitative means, obscuring the nature of their foundation and the true level of assurance they provide (Jaquith, 2007; Jansen, 2009).

• Measures may be reported out of context and without a baseline for comparison, or even simple measurements may be reported that do not show any kind of correlation, which greatly (or even completely) limits the value of the reported information (Ayoub, 2006; Jaquith, 2007).

• Complex, lower-level measures may be reduced to a "traffic-light" format, which makes measures lose many of the inherent qualities (see Section 2.2) that make them sought-after and necessary to begin with, due to oversimplification (Payne, 2006; Jaquith, 2007; Mimoso, 2009).

It can be recognized that the first two problems outlined above are, in essence, founded in the errors in measure design and development, and, in order to address these issues, the questions that the measures need to answer and the format in which the results are to be presented need to be specified ahead of time (Payne, 2006). The last problem arises from the fact that the security professionals do not always have appropriate established methods and procedures for rolling up the lower-level measures into the higher-level ones. It is generally advisable to use a tiered reporting model, with the level of specificity and technical detail gradually decreasing at each higher level and some technicalities even becoming omitted, when they do not actually facilitate decision making at the higher levels (Bartol, 2008; Pironti, 2007).
Senior management support. Possibly the most crucial factor to a successful information security metrics programme is the support and active involvement of senior management. This success factor is listed prior to the other ones in both NIST SP 800-55 (Chew et al., 2008) and ISO/IEC 27004 (ISO/IEC, 2009a); other guidance documents also highlight its importance (e.g. ITGI, 2006; 2008).

Yet, Forrester researchers assert that lack of support from senior management and difficulty of quantifying costs and benefits of security are the most common complaints conveyed by security managers (Kark, Orlov, & Bright, 2006), and it can be recognized that the former is likely to be dependent on the latter. Erroneous preconceptions and/or expectations on the part of the stakeholders may additionally have to be overcome (IATAC, 2009). The lack of a broadly accepted model/method for mapping IS metrics to organizational structure and clearly illustrating how the lower level metrics can roll up into the higher level metrics (and thus also higher level goals/objectives) in a meaningful way can possibly contribute to this problem. Without a good model or methodology for rolling up quantitative measures, security professionals often struggle to find a compromise between reporting methods that are too technical for the senior management and ones that impair the utility of a metric due to oversimplification (Mimoso, 2009).

Research Efforts

This section presents a categorized list of research efforts aimed at formalizing IS metrics, establishing better measurement practices, and addressing various associated problems and challenges. This list is by no means exhaustive but is rather intended to be illustrative and help the reader to form a holistic view of the area.

Measurement Standards

The ISO/IEC 27004 and NIST SP 800-55 measurement standards outline processes and provide general guidance for metric development as well as implementation, operations, and programme improvement. The two standards can be said to be complementary and each offers something the other does not. In brief, NIST SP 800-55 better describes the long term, strategic perspective on security measurement, factoring in the maturity and capability of an organization’s security programme, and assuming a higher level of abstraction (Chew et al., 2008). The ISO/IEC 27004 offers more detailed guidance on certain operational aspects of security measurement and is generally more formalized, while providing less of conceptual background that facilitates better understanding of the related processes. It can also be noted that the current version of the ISO/IEC 27004 standard (First Edition, December 15, 2009) contains certain errors/omissions (e.g. on the IS measurement model portrayed on Figure 5, Page 7 of the standard, the upper-left text box includes the entry "Implementation processes, procedures"; "producedures" is an apparent spelling error; even when read as "procedures", as presumably intended, the meaning of the entry as a whole is still not readily evident as it is not identified the implementation of what specifically is being referred to in this instance; considering that a large portion of the standard is based/expands on the model in question, this can be
viewed as a significant issue) (ISO/IEC, 2009a). This gives the impression that its release was rushed, possibly due to a pressing need for such a standard.

The ISO/IEC 27004 and NIST SP 800-55 standards have aided in formalization of information security metrics terminology and the common understanding and stabilization of certain related concepts. The two IS measurement standards, even when combined, do not provide comprehensive guidance on all relevant issues and at all levels of abstraction.

The ISO/IEC 15408 standard (a.k.a. Common Criteria), although having a much narrower scope and applications than NIST SP 800-55 and ISO/IEC 27004, is also relevant here as it establishes the basis for measurement of the assurance level of security provided by specific products in specific environments and, thus, can facilitate decisions concerning the suitability of products to particular organizational context/needs and can also provide a point of reference for comparing the relative levels of assurance provided by similar products (ISO/IEC, 2009b). Likewise, the FIPS 140-2 (FIPS, 2002) standard, which assumes an even narrower and more technical standpoint, can be used by organizations from a managerial perspective to the same end as the Common Criteria.

**Metrics Taxonomies**

A number of taxonomies exist that put forward high level categorizations for IS metrics. Prominent examples of classifications applicable from a management/organizational perspective include:

- **Governance, Management, and Technical** (CISWG, 2005).
- **Management, Operational, and Technical** (Savola, 2007).
- **Organizational, Operational, and Technical** (Seddigh et al., 2004; Stoddard et al., 2005).
- **Implementation, Effectiveness and Efficiency, and Business Impact** (Chew et al., 2008).
- In (CIS, 2009), though not explicitly stated, proposed metrics can potentially be categorized by their target audience, which is Management, Operations, or both (compare this to some of the previous classification examples).
Seddigh et al., Savola, and Vaughn, Henning, and Siraj, propose elaborate taxonomies consisting of multiple tiers. For illustrative purposes, only one (most applicable and easily comparable) tier of each taxonomy is listed above. Notably, Vaughn, Henning, and Siraj taxonomy includes a Technical Target of Assessment classification tree in addition to the Organizational Security one that is shown here.

While there is no single, widely accepted unified model or terminology when it comes to the categorization of information security measures, even at a high level of abstraction, some of the above do share similarities. It can also be noted that, in some of the cases, there is a tendency to separate the social and the technical facets of security.

Taxonomies are subject to inherent limitations. The categories they put forward are non-disjoint; they may overlap as well as be interrelated in some way. It can be said that taxonomies tend to simplify complex socio-technical relationships (Savola, 2007).

**Metrics Compilations**

An exceptionally comprehensive collection (more than 900) of ready-to-use IS metrics is presented by Herrmann (2007). Other, less comprehensive sources include reports such as (CISWG, 2005) and (CIS, 2009). Sample/pre-designed metrics are generally intended to be used as a point of reference for developing and tailoring metrics for organizations with young IS measurement programmes. The (CISWG, 2005) and (CIS, 2009) reports, however, attempt to establish a minimum set of core metrics that can serve as a starting point for any organization. However, outside of the groups contributing to these reports, there is, as of yet, no general consensus on what basic set of IS metrics (if any) can be considered universally applicable as different organizations can have their own distinct goals/objectives, operating environments, and may differ in terms of the capability/maturity of their IS management systems. Although, this may be more feasible to achieve across "similar" organizations. The IS metrics put forward in these reports may still serve as a good reference point for some organizations, however.

**Metrics Implementation Methods**

This section covers methodologies that are specifically meant to bridge the gaps between the different levels in an organization by providing a multi-tiered scheme for specifying measurement goals/objectives at different organizational levels and helping to derive lower-level goals/objectives from the higher-level ones, as well as facilitating reverse communication by providing a method and directions for rolling up the measurement results back to the decision makers in a meaningful way.

There are a number of advocates who are in favour of adapting the Balanced Scorecard (BSC) framework to the IS measurement and reporting purposes. For instance, ISACA supports the use of the method toward this end, and practically applies BSC in its well known COBIT framework (ITGI, 2007). A Microsoft TechNet article (Microsoft, 2007) describes how BSC can possibly be adopted for IS needs. Some other advocates include (Peuhkurinen, 2008), (Jaquith, 2007), and (Farshchi & Douglas, 2010). The applicability of BSC in this context may be debated, as it was not originally designed with information
security in mind, however, if successfully adapted to IS context, BSC can help address some of the challenges outlined previously.

Another top-down approach for prioritizing metrics is the Goal-Question-Metric (GQM) promoted by Victor Basili. GQM was developed for software engineering purposes and it has been widely adopted in that role. However, Herrmann recommends using GQM as a more broad-spectrum methodology that can be applied with an organizational viewpoint in mind (Herrmann, 2007). Furthermore, the approach has been further developed into GQM+Strategies (Basili et al., 2009), which addresses the limitations of the original and is meant to connect metrics to higher-level goals, and be applicable on all organizational levels and for different kinds of organizations.

**Advanced Measurement Methods**

Attack surface metrics constitute a promising research direction as they allow for the measurement of an entire system's security rather than individual controls. Such metrics are essentially aimed at modelling possible (and likely) attack vectors to a system with respect to attack opportunities that result from exposure of the system's attack surface (i.e. transparent and accessible actions/resources). Although, the relative complexity and lack of widespread implementation make their real-life practicability somewhat unclear.

One prominent example of such methodology was originally (informally) introduced at Microsoft, and has since been progressively developed, becoming increasingly better formalized, by researchers at the Carnegie Mellon University (Manadhata, Kaynar, & Wing, 2007). The Risk Assessment Value (RAV) methodology developed by ISECOM is another notable example. RAV, unlike the former example, which only deals with software systems, assumes notably higher abstractness and a wider scope and addresses operational security concerns in general (including physical, etc) (Herzog, 2010). Another example, based on a similar/related concept of attack graphs, is being jointly developed by researchers from NIST, the Concordia, and the George Mason universities. These efforts differ from attack surface ones in that they target networks rather than individual systems (Wang et al., 2008).

**Relevant Technologies**

The Security Content Automation Protocol (SCAP) (Quinn et al., 2009) is a collection of specifications intended to standardize the way security software solutions communicate software security flaw and configuration information. SCAP incorporates several existing standards as its components, namely, XCCDF, OVAL, CPE, CCE, CVE, CVSS, and, as of the Revision 1 version that is currently in the draft stage, OCIL. The protocol essentially constitutes an approach to automating security measurement and reporting (as well as other aspects of operational IS management). SCAP also incorporates the National Vulnerabilities Database, which is a repository of standardized vulnerability management data managed by NIST. The protocol is gradually gaining widespread support. Additional similar standards, not currently part of SCAP, by NIST and MITRE exist/are in development.
More information on these standards is available on the organizations' official websites, http://www.nist.gov and http://www.mitre.org respectively.

Dashboards are becoming a fairly common, sought-after instrument for streamlining security measurement and reporting (Kark, McClean, & Penn, 2007). The rather obvious reasons for this are that they provide a way to visualize and automate metrics reporting that operates in near real-time, and make metrics accessible in every sense of the word when properly implemented (i.e. considering the common pitfalls of metrics reporting outlined previously) (Payne, 2006; Jaquith, 2007).

**Analysis and Synthesis**

This section first reflects on the research area from a systematic perspective and then suggests a more systemic approach to structuring research in the area.

**Analysis of the Area**

The analysis outlined here reflects on the common problems and challenges found in IS measurement and prominent solutions and research efforts aimed at resolving them that were summarized in the preceding sections. The analysis is based around a simple, two-axis model outlined on Figure 1. The horizontal axis is fairly self-explanatory and represents a continuum that ranges from more practical solutions to more conceptual frameworks. The vertical axis ranges from more social (information systems) to more technical approaches. The research efforts described previously are positioned along the two axes and, while their placement is only a rough approximation, serve to illustrate an important point. The area in question is clearly multi-disciplinary in nature and is highly fractioned. While this may seem as an expected result given the dualistic nature of the model used to illustrate the issue the field of Information Security does indeed deal with complex socio-technical problems and includes both systemically and systematically inclined professionals. During the literature review it became apparent that connections between different (types of) research efforts are not always entirely clear and sometimes are clearly absent in the area.

On a more practical note, it should be acknowledged that many of the frequently encountered issues in IS measurement arise as the result of a disconnect between different administrative levels, which can be said to be situated along the "Information Systems - Information Technology" axis on the model. Metrics taxonomies and compilations, despite their attempt to cover multiple segments along that continuum, do not address this issue as they do not and cannot bridge the gaps between them in a way that would be universally applicable. The NIST SP 800-55 and ISO/IEC 27004 standards describe conceptual models but do not provide detailed methodologies for dealing with the problem. GQM+Strategies and BSC are (somewhat argumentatively, in the latter's case) designed to address the issue, but have not yet seen widespread adoption and there is as of yet no consensus methodology for implementing information security metrics across different organizational levels in a meaningful way.
Synthesis of the Area

This paper proposes that the existing dualism in IS measurement research should be turned into complementarity. A research process scheme that is able to approach the present issues in the subject area holistically is required. Figure 2 illustrates a research process by Schwaninger (2007) that integrates three pairs of dualistic concepts, Explain - Understand, Explore - Test, and Discover - Design. Relationships between the concepts are illustrated by arrows; while other relationships are possible, the ones shown here are considered to be the absolute minimum necessary for the continuance of a holistic research process.

The two main loops, Explore - Understand - Design and Design - Test - Explain are of most interest here. The former representing a systemic research approach and the latter a systematic one, combined in a complementary fashion. They also roughly correspond to the right and left sides of the graph on Figure 1, respectively. The remaining two loops represent (expected or otherwise) discovery that may unfold from exploration and/or testing.

On the example of a top-down metrics development and implementation method, the Explore - Understand - Design path leads to creation of such a method that is theoretically sound, however, creating a theoretically sound model and a practical one are not the same. Consequently, Test - Explain - Understand steps follow, after which the
Conceptual design can be improved upon based on the acquired feedback in order to be more in line with the practical realities of security management. The outlined path does not have to keep repeating itself, however. A key feature of the scheme is that the path can alternate after each cycle as necessary, which results in a research approach that is conducive to interdisciplinary modes of operation.

![Diagram](image)

Figure 2. A systemic scheme for the research process (Schwaninger, 2007).

Conclusion

This paper presented some of the key findings of a comprehensive literature review on the subject of information security measurement. Basic concepts, common problems and challenges, and prominent examples of current research efforts were outlined. It was shown that the research efforts in the area are somewhat segregated due to their interdisciplinary nature. A possible research approach was outlined that can facilitate interdisciplinary modes of operation in the area. While interdisciplinary research is neither especially common nor easy, information security professionals are often faced with socio-technical questions that cannot be solved or answered by addressing only one half of the problem.

References


