Modelling Static and Dynamic Aspects of Security: 

A Socio-Technical View on Information Security Metrics

Stewart Kowalski, Rostyslav Barabanov 
Department of Computer and System Sciences, Stockholm University 
Kista, Stockholm 164 40, Sweden 

ABSTRACT

Managing something that is not measured is difficult to near impossible and information security is not an exception. In the recent years, this has become increasingly apparent.

Noticeable progress has been made in advancing the areas of information security measurement and reporting. However, a number of challenges and gaps still remain, and the existing paradigms meant to address them are not without limitations.

In this paper, we suggest a socio-technical model that was previously used to model USA's national computer security policy as a model that can be applied to the information security metrics area. The model can provide a unifying, holistic view on the area, illustrating interrelationships and gaps between various efforts at different abstraction levels. The proposed model can be mapped to some of the existing paradigms and, possibly, help address some of their individual limitations by offering a more unified perspective.


1. INTRODUCTION

To paraphrase the frequently quoted 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 difficult to near impossible.

This realization has become increasingly apparent in the area of information security over the past decade. For instance, a fairly recent survey by Frost & Sullivan showed that the interest (and need) for information security metrics was high and on the rise among the (more than 80) surveyed companies [1]; while, in a global survey sponsored by ISACA, dependable metrics were perceived to be one of the critical elements of an information security programme's success by many executives and security professionals [2].

Possibly the greatest driver for these developments for most organizations is the recently amplified regulatory environment that demands 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 their information security programmes.

As a consequence, a number of related 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 information security metrics. A recent state-of-the-art report on the subject [3] shows that, although numerous advances have been made in the last ten years, in several respects the area is still in its infancy.

There are still a number of open issues in the area in question and numerous knowledge, methodology, and technology gaps still remain. The particular issue that we wish to focus on here, however, is modelling of information security metrics from a socio-technical perspective (and the current lack thereof) that provides a holistic way of looking at the area, while illustrating interrelationships and gaps between various specific efforts at different organizational/abstraction levels.

The next section provides an extended problem statement and additional background information. Section 3 introduces our proposed solution (model). Finally, Section 4 reflects on the preceding sections and the suggestions future research activities.

2. EXTENDED BACKGROUND

In order to better describe the problem, in this section we will examine and outline the common challenges encountered in information security measurement and reporting, and existing paradigms/models intended to address them.
Firstly, it must be realized that success of a security metrics programme is highly dependent on good governance and the active involvement of management at all echelons within the organization, and starting at the highest level. This has been established and emphasized in numerous sources (e.g. [4] [5] [6] [7]). There are, however, challenges to this.

Information security managers often struggle with gaining the upper management support [8][9] and overcoming unrealistic expectations on their part [3]. Finding out what to measure as well as how to report it in a manner that is meaningful to the upper management is also a common problem [1][10][11][12] that often results in reporting of information that is not useful for strategic decision making.

It can be recognized that the above largely occur due to a lack of consensus on how to communicate security measurement related issues between different organizational layers. This is often compounded by the fact that the social/management and the engineering/technical sides inherently tend to view things from two different perspectives and do not always "speak the same language", while it is necessary to "roll up" lower-level, more technical metrics into higher-level ones in a meaningful way across organizational levels.

In recent years, a certain level of consensus has been reached with regards to the security measurement related terminology and vocabulary [3], partly due to the NIST SP 800-55 [7] and ISO/IEC 27004 [6] security measurement standards. There is, however, no broad consensus on how to classify and structure different (layers of) security metrics, which often leaves the security professionals without a definitive model or paradigm that can be used to map security measurement efforts to their organizations and establish a meaningful connection between metrics at different levels. Below, we will briefly outline and discuss some prominent attempts at the latter, dividing them into two types, which may be called static (metric taxonomies and classifications) and dynamic (metric development and/or selection approaches).

**Taxonomies/Classifications**

The purpose of taxonomies is to organize the different classes they contain in a manner that is both comprehensive and non-redundant. The following list includes some of the prominent examples of high-level classifications of security metrics that have been put forward in the last decade.1

- **Governance, Management, and Technical** [13].
- **Organizational, Operational, and Technical** [14].
- **Management, Operational, and Technical** [15][16].
- **(Information Assurance) Programme Development, Support, Operational, and Effectiveness** [17].
- **Organizational and Performance, Business Value, Business Process, Operational, Technological, and Compliance** [18].
- **Implementation, Effectiveness and Efficiency, and Business Impact** [7].
- **Classification of security metrics using a Balanced Scorecard based taxonomy, that is, into Financial, Customer, Internal Business Processes, and Learning and Growth**, also has some proponents [11].

It can be seen that all of the above attempt to classify or, in a sense, model information security metrics with regards to the structure and/or information needs of organizations in a way that is meaningful for practical purposes. The NIST example above [7] stands out from the rest in that it classifies security metrics based on the degree of security programme maturity needed to effectively implement them.

However, taxonomies possess certain inherent limitations that restrict their usefulness. Namely, they do not identify/explain interrelationships between classes. Within the context of this paper, it can be acknowledged that taxonomies tend to oversimplify complex socio-technical relationships [16].

Several of the above simply separate the social and technical metric classes. It is, however, possible for a metric to be both (e.g. reduced number of malware on an organization's internal network may be due to effective technical controls, but also strict workstation use policies and higher security awareness among employees, for instance; an aggregate metric meant to measure the correlation between these factors would have no place in several of the above taxonomies). This causes a clear disconnect between the social and technical facets of security that only increases when any additional layers of metrics are introduced.

As was previously stated, it is necessary to be able to roll up lower-level metrics into higher-level metrics in a meaningful way. Security metrics taxonomies are not conductive to this and there is a need for models/paradigms that are.

An ontology may possibly serve as a solution to this problem. However, we could not find any existing (complete) security metrics ontologies as of the time of this writing. It can also be argued that an ontology will either be too incomprehensible or
too complex to be practicable and that a more abstract model may be needed.

**Development Approaches**

Development and/or selection of what to measure and report can be done with either a top-down or a bottom-up approach. The key advantage of the latter is easier identification of what is more feasible to measure, while the former provides a better means for deriving the lower-level objectives from the higher-level ones [12]. It is commonly recognized, however, that one of the major issues in the security measurement and reporting areas is that reported information is often based on what is easier to measure rather than on what is actually more meaningful strategically (e.g. [5] [9] [11] [20]). This seems to indicate that the advantages the top-down approaches provide outweigh the ones provided by the bottom-up ones.

The NIST SP 800-55 [7] and ISO/IEC 27004 [6] information security measurement standards both provide process models for metrics development that operate in a top-down, iterative fashion (i.e. they include feedback loops/channels). The GQM (Goal Question Metric) paradigm, although initially designed with a purely engineering point of view in mind, can arguably also be applied from an organizational perspective [20], while the GQM+Strategies [21] extension was designed specifically with this context in mind. There are also proponents of using the Balanced Scorecard framework in this capacity [11].

Top-down metrics development processes can essentially be used to devise the lower-level metrics based on higher-level objectives, and to set up a line of communication that allows metric and measurement process revisions based on feedback and facilitates reporting of what is relevant at the given level. However, neither NIST SP 800-55 nor ISO/IEC 27004 offer comprehensive guidance on how to roll up metrics across the organizational levels (while they do acknowledge the general possibility).

While top-down oriented metrics development processes are useful for creating organization and context specific metrics, without a static component, they have limitations of their own. Taxonomies can still be more useful in devising standardized sets of reference metrics that can be shared and reused across organizations or be used in inter-enterprise benchmarking, for instance.

It can be recognized that the balanced scorecard framework incorporates both static and dynamic elements. However, it is not inherently designed to be used in the information security context, nor in all types of organizations for that matter. This makes its applicability disputable.

NIST SP 800-55 also has both static and dynamic elements as mentioned above, but it does not provide a model for dealing with metrics and their interrelationships at different abstraction or organizational levels.

### 3. A SOCIO-TECHNICAL MODEL

In this section, we introduce a socio-technical model that can provide a unifying, holistic view on the topic area, illustrating interrelationships and gaps between various related efforts at different levels of abstraction.

**The SBC Model**

The proposed model was first published in 1991 and, notably, was previously successfully used to model the United States national computer security policy [22]. The main purpose of the model can largely be derived from its name, Security By Consensus (SBC), and is to facilitate formation of consensus among various stakeholders of an information system, while bearing in mind their different frames of reference. The SBC model can be illustrated as follows:

![SBC Model Diagram](image)

**Static Classes**

- Ethical
- Cultural
- Legal
- Political
- Administrative
- Managerial
- Operational
- Technical

**Dynamic Classes**

- Principles Development
- Policy Decision Making
- Requirement Specification
- Implementation
- Testing Evaluating

As can be seen on Figure 1, the SBC model incorporates two classification schemes, one static and one dynamic.

The dynamic classes represent the dynamic states of the static classes and follow an ideal (i.e. "perfect", but not necessarily realistic) process development model. In this model, there are feedback loops (only) between the adjunctive classes. Lack of additional, more direct feedback loops is due to the fact that there is tendency for rapid feedback loops in social systems to

---

2 For a detailed account of the SBC model history, validation efforts, and analysis methodology, see the reference.
cause instability [23]; the *ideal* model is designed as to avoid this.

The static classes comprise a layered model of an information system, where each layer constitutes a function. All the layers follow the same development model with five dynamic states and it is suggested that a certain level of synchronicity among the dynamic states of the static classes is required in order to facilitate/maintain stability in the system (e.g. implementing policies that are not reinforced by relevant laws or ethics may not have the desired outcome).

The static classes are interrelated, and are joined by semantic and syntactic chains where, *ideally*, but again not necessarily, the higher layers give meaning to the lower ones (e.g. policies give meaning and serve as basis for procedures).

**SBC And Metrics**

We propose that it is possible to adapt the SBC model to the information security metrics from the organizational point of view. This can be accomplished as follows.

Firstly, it can be recognized that the static classes in the SBC model share certain similarity with some of the classifications introduced in section 2. Classifications schemes such as [14], [15], and [16] map directly onto the three lower layers in the model, and some of the other listed schemes can be partially mapped to the model if unchanged and completely with some changes to the classes. For the sake of simplicity, we will use the schemes that can be mapped directly in this argument.

The high-level classifications listed in section 2 are essentially “flat”, that is, they are all located at the same abstraction level. By mapping them to the SBC model, we indicate a connection between them as per previously described rules of the model (e.g. the syntax of the *operational* class is derived from the semantics of the *managerial* class; in other words, metrics classified as operational are based on the managerial ones).

The two remaining static classes, cannot be directly controlled from an organizational perspective, but constitute the ethical (cultural) and legal context in which the organization operates and, therefore, still influence the lower layers as expected.

A metrics development/selection process model, such as the ones outlined in ISO/IEC 27004 and NIST SP 800-55 metrics standards can be implemented within each of the three lower static classes.

The dynamic states of the three lower layers can then be used for determining the degree of synchronization between them across these layers as well as the upper two, representing the legal and ethical/cultural environment.

**4. CONCLUSION**

In the 1991 study of United States (US) national computer security policy it was found that there was unsynchronised and intrinsically unstable framework in place in the US. It appears that with the current state of practice [3] in the US that the 2002 Federal Information Security Act has had similar consequence on security metrics development as the 1987 Computer Security Act. That is to say that it in order for the system to maintain itself securely a great degree of active intervention and communication is required. This intervention and communication works at a national level. However given the current global interconnectivity of information systems it is necessary that information security measurement be modelled using a socio-technical view in order to develop more efficient and secure global communication infrastructure.

**5. REFERENCES**


