Assessing the Feasibility of Security Metrics

B. Heinzle and S.M. Furnell

Centre for Security, Communications and Network Research
Plymouth University, United Kingdom
e-mail: info@cscan.org

Abstract

Security metrics are used to measure the effectiveness of an organisation's Information Security Management System (ISMS) as well as the sub-processes, activities and controls of the ISMS. Guidelines and example metrics have been published, but it is still difficult for an organisation to select metrics that are feasible for their environment, i.e. their ISMS.

This paper proposes a self-assessment framework that allows a user to determine security metrics that are feasible specifically for the user's ISMS. To achieve this, a metric catalogue containing 95 metrics from different sources was created. For each metric, requirements that need to be fulfilled in order to be able to use the metric, and ISO 27001 clauses and controls whose effectiveness is being measured by the metric, were ascertained and assigned. By this, a list of requirements was generated that can be used to describe an organisation's ISMS. During an assessment, the user indicates which requirements from the list of requirements are fulfilled. After conducting an assessment, a list of feasible metrics, the number of metrics per ISO 27001 clause and control, and other information are generated as assessment results. A software prototype was created and shows a proof of concept of the self-assessment framework. The results of the study were evaluated by external experts, which has shown the usefulness of the study and helped to identify areas of improvement and future work.

Keywords

Security Metrics, Security Measurement, Feasibility, Effectiveness, ISMS

1 Introduction

The term metric in general stands for the process and methods of quantification of a given attribute, aspect or characteristic (Savola, 2007; Jansen, 2009). Savola (2010) states that metrics "[...] simplify a complex socio-technical system into models and further to numbers, percentages or partial orders". According to this definition, information security metrics measure aspects of information security.

While security metrics are defined differently and can be categorised differently (Chew *et al.* 2008; COBIT5, 2012; Savola, 2007; Saydjari, 2006; Jansen, 2009), this study focuses on security metrics according to ISO 27004 (2009): Metrics that measure the effectiveness of an ISMS and its sub-processes and controls. A variety of frameworks and guidelines on how to set up a so called information security measurement programme exist (ISO 27004, 2009; Chew *et al.* 2008; COBIT5, 2012; Payne, 2006), although these publication only give little or no guidance on how to select the most feasible or adequate security metrics.

Further publications in the area of security metrics mostly agree that security metrics are a difficult area and further research is strongly needed (Bellovin, 2006; Hinson, 2006; Jansen, 2009; Rosenquist, 2007; Saydjari, 2006). Two approaches for determining feasible security metrics were reviewed. Savola's (2010) approach is a set of evaluation criteria with a scheme how to evaluate candidate metrics according to this scheme. Fruehwirth *et al.* (2010) published an approach that tries to determine feasible metrics by considering the organisation's capabilities according to the Systems Security Engineering Capability Maturity Model (SSE-CMM).

2 Possibilities to describe an ISMS

For the self-assessment framework that was developed during this study a formal method to describe an organisation's ISMS is vital in order to enable the determination of feasible security metrics. Rather than evaluating a list of security metrics from a catalogue and determine the best suitable or most feasible metrics according to an evaluation scheme such as Savola's (2010) approach, a method to describe an organisation's ISMS and determine feasible metrics with the information about the ISMS was researched.

Similar to the approach published by Fruehwirth *et al.* (2010), the maturity model used in CobiT 4.1 (2007) and the ISO/IEC 15504 based process capability model used in COBIT5 (2012) were reviewed. One further possibility to describe an organisation's ISMS offer catalogues of possible elements of an organisation's ISMS such as the "IT-Grundschutz Catalogues" (BSI IT-Grundschutz Catalogues, 2005). It was evaluated how the existence of specific components could indicate that specific metrics are feasible.

While reviewing process capability or maturity models and modelling catalogues towards their usefulness to describe an ISMS with the aim of determining feasible security metrics, both possibilities were not considered suitable for the self-assessment framework. This was mainly because establishing a link between metrics and certain elements of the reviewed possibilities or attributes of these elements seems to be difficult. Also using these possibilities would limit organisations that can use the self-assessment framework to those organisations that use the relevant method to describe an ISMS or manage IT in general.

It was decided to use a method that is closer oriented to metrics and less bound to ISMS frameworks like ISO 27001 (2005) or the COBIT process capability and maturity model (CobiT, 4.1 2007; COBIT5, 2012). To describe an organisation within the self-assessment framework, requirements of each metric were worded without using a predefined model or formal language. Requirements are described as a condition that needs to be fulfilled by components of the ISMS or information that needs to be reported by components of the ISMS, e.g. "Inventory of assets indicates number of applications that are classified as critical to the organisation". The list of recorded requirements can then be used to build an organisational model. An organisation shall be described by the list of fulfilled requirements, which will be a subset of the overall list of requirements.

3 Metrics Catalogue

A metric catalogue was created and contains the following information:

- Source of the metric
- Title of the metric
- An identifier which is unique within the source
- Brief description, e.g. "Percentage (%) of information systems that have conducted annual contingency plan testing"
- ISO 27001 processes and controls that are measured by the metric: At the end of an assessment, this allows to determine which controls are measured.
- Requirements of the metric, i.e. a condition that needs to be fulfilled for the metric to be feasible.

An overview of sources and the number of metrics used from each source is shown in Table 1.

ISO 27004 (2009)	13
NIST SP 800-55 (Chew *et al.* 2008)	16
Steve Wright (2006)	7
The CIS Security Metrics (The Center for Internet Security, 2010)	28
Scott Berinato (2005)	5
Robert Lemos (2012)	4
COBIT5 (2012)	13
security metametrics blog (Brotby and Hinson, 2012)	9
total number of metrics	95

Table 1: Number of metrics per source

The list of ascertained requirements was grouped into categories of requirements. Categories were made based on the area of the ISMS or the IT activities that are addressed. Categories are similar to ISO 27001 control sections or control objectives. Furthermore, for each ISO 27001 clause and control the number of metrics that measure it can be determined, as relevant clauses and controls were assigned to each metric.

4 Self-Assessment Framework

Figure 1 shows an overview of the developed self-assessment framework, the data that is being used and how this data correlates.

As initial data the framework uses the metrics catalogue, the list of requirements, a list of ISO 27001 clauses and controls and the relationships between these three items, which are again stored in the metrics catalogue.

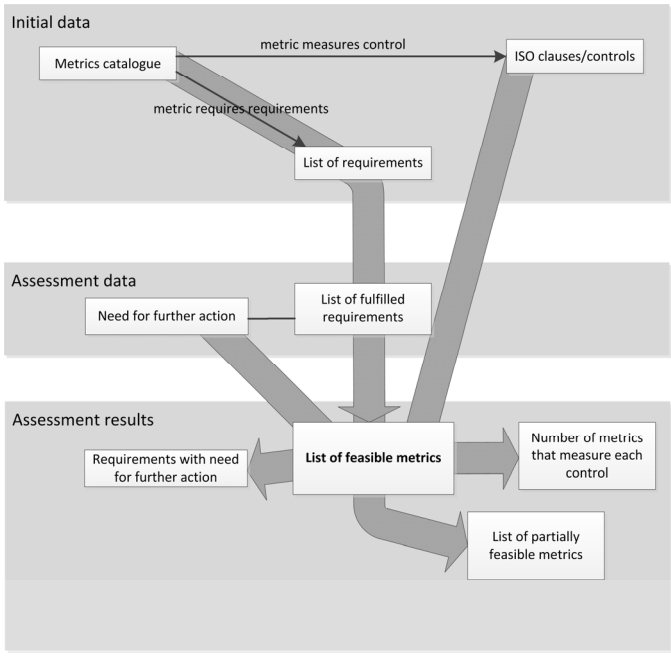

Figure 1: Self-assessment framework

During an assessment, the user is asked to indicate which of the requirements are fulfilled within the ISMS. It might occur that a requirement is currently not fulfilled properly, but fulfilment can be achieved in near future. If this is possible with a reasonable effort and the user is willing to do so, the user can indicate this for each fulfilment of a requirement. In this case, the requirement is considered as fulfilled to the effect that the metrics that rely on this requirement are considered feasible as long as the metric's other requirements are fulfilled. Comments on how the requirement will be fulfilled in future should be added for documentation purposes. The opportunity to add comments on the possibilities and modalities of data collection related to each requirement is given to the user.

Once the user has walked through the list of requirements and has indicated which requirements are met, the following assessment results can be determined: (1) A list of feasible metrics, i.e. metrics that have all their requirements fulfilled. If one or more requirements of a metric need some further action in order to be fulfilled properly, the metric is still considered feasible. (2) A list of requirements that need further action to be fulfilled properly, i.e. all the requirements for those it was indicated the requirement is currently not fulfilled but fulfilment will be achieved with reasonable effort in near future. All issues on this list should be addressed by the user of the framework. (3) A list of partially feasible metrics, i.e. some but not all the requirements were fulfilled. This list indicates which metrics could be used if more requirements were fulfilled. (4) A list showing ISO 27001 clauses and controls with the number of feasible metrics per clause and control is generated. In this way, the user of the framework sees at a glance of which clauses and control the effectiveness can be measured.

With the aim of providing an example how the self-assessment framework could be used in practice, a software prototype was implemented. This was achieved using Microsoft Access 2010. The software prototype offers functionalities for editing the metrics catalogue and the list of requirements as well as conducting assessments. Reports for metrics (i.e. the metrics catalogue), requirements and assessments can be generated as well.

5 External Evaluation and Discussion

The results of the study were evaluated by 11 external experts. Evaluators are working in the following positions: Professor at University of Applied Sciences Upper Austria, CISO at Domestic & General, Manager at a leading Security Consulting Company in London, Sr. IT Auditor at General Motors UK, Security Manager at HCL Great Britain Ltd, GRC Consultant in InfoSec at RNG Conseil Limited, Digital Security Risk Consultant at BP, Information Security Manager at Marie Curie Cancer Care, Audit Manager at Cofunds Limited, Security Manager at Hermes Fund Managers Limited as well as a Risk and Compliance Manager from a further UK-based company. The evaluation was done by asking for the evaluators' opinions about the metrics catalogue, the list of requirements, the self-assessment framework (as a theoretic description) and the software prototype via 13 questions.

In general, the evaluated components were found very useful. Some proposals for improvement were made. Besides different presentation formats and grouping for the catalogue and the list of requirements, a more detailed description of the self-assessment framework and improvement of the prototype's usability, comments mostly proposed new metrics as well as new functionalities and ways how the framework and the software prototype could be developed further. However, many of these proposals were related to extending the software to support data collection and calculation of metric results as well. The results of the study leave room for further development, but these proposals address functionalities that were not part of the original aims of the study. It was also commented that metrics should be linked to business objectives and then be selected according to the metric's ability to fulfil relevant objectives, as it is done by other publications (Chew *et al.* 2008; Fruehwirth *et al.* 2010; ISO 27004, 2009). Nevertheless, metrics are linked to control objectives, which can be seen as a certain type of business objectives. Although the framework in its current version does not select metrics according to a list of ISO 27001 control objectives that shall be achieved, it is possible to adapt both framework and software prototype to allow this.

Some metrics were found as infeasible or very unlikely to be fulfilled. This is known and shall not be considered as a weakness. Metrics can be added to the catalogue, even though their requirements are very infeasible, as long as their requirements were ascertained and worded correctly. This solely results in the metrics being feasible during hardly any assessment.

In order to draw a line between the framework and the software prototype, in can be said that the framework is the theoretic approach of using the metrics catalogue (including the requirements per metrics) and determining feasible metrics for a customer by using the entire list of requirements and indicating which metrics are

fulfilled. The prototype is a software implementation of the framework, but the idea behind it resides with the framework. That means that it is not necessary to use the software prototype in order to use the framework, one could make a different implementation or do it manually with paperwork. The self-assessment framework and the software prototype are not the same thing but the software prototype is strongly linked to the framework.

While ascertaining requirements it was found that the feasibility of metrics depends heavily on the support given by software used for patch, asset, incident, identity, etc. management. This finding also reflects that some of these software solutions fully integrate the calculation of security metrics.

6 Conclusion and Future Work

The metrics catalogue delivers an extensive set of metrics for measuring the effectiveness of an ISMS or processes and controls of an ISMS. The catalogue's use is not limited to the self-assessment framework; it can be used independently as a collection of security metrics. The catalogue is not only a collection of security metrics, also ISO 27001 clauses and control were assigned to each metric if their effectiveness is being measured. As essential information for the self-assessment framework requirements were ascertained for each metric. The metrics catalogue does not and could never claim completeness. As used sources can change or new sources can appear, constant monitoring of existing sources and updating of the catalogue is needed.

The self-assessment framework defines how feasible metrics can be determined. An assessment is conducted by presenting the list of requirements to the user, who indicates which requirements are fulfilled by the user's ISMS. Results of the assessment are not only feasible metrics: a list of partially feasible metrics can be created together with an action plan indicating which requirements need further action to be fulfilled properly and the number of feasible metrics per ISO 27001 clause and controls, which has the benefit that the user of the framework sees at a glance which parts of the ISMS have their effectiveness measured. With the self-assessment framework, anybody can determine feasible metrics; no special knowledge regarding security metrics is needed. The only requisite is being sufficiently informed about the ISMS or having enough information about the ISMS at disposal so that one can indicate which requirements are fulfilled.

The software prototype provides a proof of concept of how an assessment according to the self-assessment could be conducted with tool support. Additionally, the software prototype allows management of all data needed by the self-assessment framework and generates documents such as the metrics catalogue. The software prototype is rather a proof of concept than a piece of software that is ready for release. Further work is needed before releasing it to the market. The framework and the software prototype could be developed further by adding graphical charts to the reports, allowing users to adapt metrics, include processes from data collection to presentation of metric results and offering more interactive methods than PDF files to explore data like the metrics catalogue or the assessment results.

The external evaluation showed the usefulness of the results of the study and additionally helped to identify limitations and future work.

Similar as the reviewed other approaches for selecting metrics, this approach still relies on subjective perceptions of individuals. The ascertainment of requirements for each metric involves subjectivity. In addition, the assignment of controls to security metrics was done mainly based on the perception of the researcher. The metrics catalogue and in particular mappings to controls and requirements could be revised in a peer review process.

The reviewed frameworks and guidelines for establishing an information security measurement programme offer little guidance on how to select metrics. Therefore, the self-assessment framework could be integrated into those frameworks. Any source of metrics could list the requirements per metric and enable users to determine feasible metrics via the self-assessment framework and the software prototype.

7 References

Bellovin, S. (2006), 'On the brittleness of software and the infeasibility of security metrics', *Security & Privacy* **4**(4), 96–96.

Berinato, S. (2005), 'A few good information security metrics'. http://www.csoonline.com/article/220462/a-few-good-information-security-metrics [Accessed 5 May 2012]

Brotby, C. and Hinson, G. (2012), 'Security metametrics: SMOTW: Security metrics of the week'. http://securitymetametrics.blogspot.co.nz/search/label/SMotW [Accessed 23 Jun 2012]

BSI IT-Grundschutz Catalogues (2005), Bonn. Federal Office for Information Security (BSI). https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutzcatalogues_node.html [Accessed 12 Dec 2011]

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A. and Robinson, W. (2008), *NIST Special Publication 800-55: Performance Measurement Guide for Information Security*, National Institute of Standards and Technology, Gaithersburg. http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf [Accessed 15 Dec 2011]

CobiT 4.1 (2007), Illinois. IT Governance Institute. http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT_4.1.pdf [Accessed 10 Dec 2011]

COBIT5 (2012), Illinois. A Business Framework for the Governance and Management of Enterprise IT. ISACA. http://www.isaca.org/COBIT/Pages/Product-Family.aspx [Accessed 16 May 2012]

Fruehwirth, C., Biffl, S., Tabatabai, M. and Weippl, E. (2010), Addressing misalignment between information security metrics and business-driven security objectives, *in* 'Proceedings of the 6th International Workshop on Security Measurements and Metrics', MetriSec '10, ACM, New York, pp. 6:1–6:7.

Hinson, G. (2006), 'Seven myths about information security metrics', *The Information Systems Security Association ISSA Journal July 2006* (July), 1–6.

ISO 27001 (2005), Genf. ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization (ISO).

ISO 27004 (2009), Genf. ISO/IEC 27004:2009 – Information technology – Security techniques – Information security management – Measurement. International Organization for Standardization (ISO).

Jansen, W. A. (2009), *Directions in security metrics research*, National Institute of Standards and Technology, Gaithersburg. http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf [Accessed 25 Dec 2011]

Lemos, R. (2012), 'Five strategic security metrics to watch'. http://www.darkreading.com/security-monitoring/167901086/security/perimeter-security/232601457/five-strategic-security-metrics-to-watch.html [Accessed 20 May 2012]

Payne, S. C. (2006), *A Guide to Security Metrics*, SANS Institute. http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55 [Accessed 17 Dec 2011]

Rosenquist, M. (2007), 'Measuring the return on it security investments'. http://communities.intel.com/docs/DOC-1279 [Accessed 12 Feb 2011]

Savola, R. (2007), Towards a taxonomy for information security metrics, *in* 'Proceedings of the 2007 ACM workshop on Quality of protection', QoP '07, ACM, New York and NY and USA, pp. 28–30.

Savola, R. (2010), 'On the feasibility of utilizing security metrics in software-intensive systems', *IJCSNS International Journal of Computer Science and Network Security* **10**(1), 230–239.

Saydjari, O. S. (2006), Is risk a good security metric? , *in* 'Proceedings of the 2nd ACM workshop on Quality of protection', QoP '06, ACM, New York, pp. 59–60.

The Center for Internet Security (2010), 'The CIS Security Metrics'. https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf [Accessed 29 Nov 2011]

Wright, S. (2006), 'Measuring the effectiveness of security using ISO 27001'. http://wwww.iwar.org.uk/comsec/resources/iso-27001/measuring-effectiveness.pdf [Accessed 1 Jul 2012]