Software Engineering
2016; 4(4): 59-64
http://www.sciencepublishinggroup.com/j/se
doi: 10.11648/j.se.20160404.11
ISSN: 2376-8029 (Print); ISSN: 2376-8037 (Online)

Review Article

Overview of Security Metrics

Rana Khudhair Abbas Ahmed

Computer Techniques Engineering Department, Al Rafidain University College, Baghdad, Iraq

Email address:
rana_ruc@yahoo.com

To cite this article:
Rana Khudhair Abbas Ahmed. Overview of Security Metrics. *Software Engineering.* Vol. 4, No. 4, 2016, pp. 59-64.
doi: 10.11648/j.se.20160404.11

Received: October 29, 2016; **Accepted**: November 9, 2016; **Published**: December 5, 2016

Abstract: Metrics are tools that are designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. This paper provides an overview of the security metrics and its definition, needs, attributes, advantages, measures, types, issues/aspects and also classifies the security metrics and explains its relationship with risk management.

Keywords: Security, Metrics, Advantages, Information, Measurement

1. Introduction

The term “security metrics” is used often today, but with a range of meanings and interpretations. “Metrics are tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. The purpose of measuring performance is to monitor the status of measured activities and facilitate improvement in those activities by applying corrective actions, based on observed measurements. While a case can be made for using different terms for more detailed and aggregated items, such as ‘metrics’ and ‘measures,’ this document uses these terms interchangeably. "Measurements provide single-point-in-time views of specific, discrete factors, while metrics are derived by comparing to a predetermined baseline two or more measurements taken over time [1].

Measurements are generated by counting; metrics are generated from analysis. In other words, measurements are objective raw data and metrics are either objective or subjective human interpretations of those data". For information system security, the measures are concerned with aspects of the system that contribute to its security. That is, security metrics involve the application of a method of measurement to one or more entities of a system that possess an assessable security property to obtain a measured value [1].

Measurements provide single-point-in-time views of specific, discrete factors, while metrics are derived by comparing to a predetermined baseline two or more measurements taken over time.

Measurements are generated by counting; metrics are generated from analysis. In other words, measurements are objective raw data and metrics are either objective or subjective human interpretations of those data. The method of measurement that is employed should be reproducible, and should achieve the same result when performed independently by different competent evaluators. Also, the result should be repeatable, so that a second assessment by the original team of evaluators produces the same result. A method of measurement used to determine the unit of a quantity could be a measuring instrument, a reference material, or a measuring system [1].

The measurement of an information system for security involves the application of a method of measurement to one or more parts of the system that have an assessable security property in order to obtain a measured value of measurements should be timely and relevant to the organization [1].

2. Related Work

[2] Presented a brief overview of the metrics, discussed how the metrics were derived, and provided an example of categorizing them. He focused on the perspective of a systems security engineering services provider, who is applying in house SSE-CMM metrics associated with some of the process areas. The purpose is to assess no only the provider’s own risk

management capability, but also the client's capability to provide good security risk management services to end-users.

[3] Presented a case study performed at a Swedish government agency. The aim of the study was to evaluate a method for the design and implementation of information security metrics. The used method was based on the method outlined in the standard ISO/IEC 27004 augmented with a participatory design approach. The standard provided a template for the specification of metrics, whereas the augmentation is essential in order to extract the information needed from the agency in order to be able to design the metrics. [4] Examined the present state of the art of information security measurement from an organizational standpoint with enough relevant information so as to facilitate a holistic understanding of the area. [5] Reviews and compares existing scientific approaches and discusses the relation between security investment models and security metrics**.**

3. Information Security Metrics' Concept

3.1. Definition of "METRICS"

Understanding the different metrics available for information security starts with a recall of what a metric is. The Oxford online dictionary defines metric as a system or standard of measurement. And it defines measurement as the action of measuring something, the action of ascertaining the size, amount, or degree of (something) by using an instrument or device marked in standard units [6, 7, 8, 9]. Metrics and measurement are intimately linked. Although they are often used one in place of the other, they are different. In the rest of this paper, the option has been made to use them interchangeably, in adoption of a posture similar to the one of Applied Computer Security Associates (ACSA) [6, 10]

Metric is usually presented as an abstract, a subjective attribute [6, 11], while a measure is a concrete, objective attribute. Measurement results from an observation, using some appropriate method to collect data and metric represents the observed data in kind of scale [6, 12]. After making observations to realize measurements, analysis is performed to generate metrics [6, 13].

3.2. Metrics vs. Measurements

There does however seem to be a common understanding that measurements is about making observations [14, 15] and that these are at a single point in time [14, 16]. Metrics on the other hand are about analysis and comparison [10, 1]. They are supposed to give you information about IT Security [14, 17]. Andrew Jaquith de_nes metric as being a standard of measurement [14, 18]. The standard ISO/IEC 27004 defines measurement as the process of obtaining information about the effectiveness of Information Security Management System (ISMS) controls [14, 4]. The same standard defines measure as being a variable to which the result of a measurement is assigned. The term indicator is also something that comes up in the literature in relation to metrics [14].

3.3. What Constitutes "Good" Metrics

A number of different publications on the subject, including standards, frameworks, and various books and articles by independent experts recommend that, in order to properly serve their intended purpose, information security metrics should possess certain "ideal" characteristics. One of such sets of ideal characteristics (Jelen, 2000), originally coined by John Wesner and sometimes cited by other sources, advises that metrics should be "SMART", that is, specific, measurable, attainable, repeatable, and time-dependent. Some other examples of proposed definitions of ideal security metric characteristics include accurate, precise, valid, and correct (Herrmann, 2007); meaningful, reproducible, objective and unbiased, and able to measure progression towards a goal [4, 19 Chapin & Akridge, 2005], consistently measured, cheap to gather, expressed as a cardinal number or percentage and using at least one unit of measure, and contextually specific [4, 20].

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 [4]:

- 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

3.4. Needs for Security Metrics

The technological explosion nowadays forces organizations to change their functioning and structures. Technology becomes the main factor for productivity growth and organizations' competitiveness and allows effective cost reductions. The use of technologies, their role and importance are increasing more and more by day. The current hefty globalization and de-localization phenomena should not be ignored any more. Organizations externalize their production activities more and more following a so called "company without factory" model. Thus, an organizations' communication center becomes increasingly important as they are depending more on their information system then they did in the past. A dysfunction of such center can paralyze

all the system and could have disastrous consequences for the company at many levels (financial, reputation etc.) [21].

The risk of paralysis could be even more critical for companies whose principal asset and added value is information. A typical highly vulnerable sector for such risks is for example the services sector. Security issues within an organization must therefore be treated as a priority at top managerial level [21].

3.5. Why Measuring Information Security

Usually, when available, cyber strategies state visions to protect economies. At the level of transformation of that vision of improving information security into facts, at the point of implementation of those wills, there are many solutions, many options. And the permanent question is to know to what extend all initiatives are pertaining, are effective, and are efficient. It is about knowing and being able to demonstrate that the actions have lead from a level B of information security to a level C or D, which is supposed to be better. Measuring information security using consistent metrics improves ability to understand it and control it. Information security metrics offer opportunity to identify sources of security data, to assert the pertinence of security data in alignment with the business, to associate numbers to activities that have been traditionally hard to measure [6].

3.6. Is Security Measurable

Wondering if security is measurable is a genuine question. Like attributes such as beauty, scent, or flavor, or factors such as motivation and intent, security is intangible. Security offers then very few mean to operate any direct measurement. Security is an abstraction, a concept, an idea, a notion, as opposed to a fact or a material consideration. So far, measuring intangible happens very often. Teachers are measuring their student knowledge when they grade them; managers are measuring their staff performances when they grade them, IT professional's measure “strategic alignment”, “customer satisfaction”, “employee empowerment” or “improved performance” as benefits of IT projects when presenting them for decision of top management. Douglas Hubbard [6, 22] is even stating that “everything is measurable”. When he says that he hasn’t found a real ‘immeasurable’ yet, he has developed, among many, measure of the risks of cyber-attacks [6].

3.7. Metric Lifecycle

The business logic associated with a metric follows a simple processing pattern [1]:

- Create: Obtain primary input data from one or more authoritative providers, including commercial products or homegrown customer applications.
- Calculate: Apply a series of analytic operations (called actions) on the primary data to derive a result and store the result in the metric results database in the form of one or more rows in a table.
- Communicate: Communicate the metric results in any of the following formats: default visualization, email notification, email alert based upon detection of some policy violation.

3.8. Issues/Aspects of Security Measurement

Insights into some critical aspects of security measurement are discussed below. The purpose is not to give a list of common pitfalls rather the objective is to highlight those factors that are believed to be pertinent to a research effort in security metrics [1]:

(1). *Correctness and Effectiveness:* Correctness denotes assurance that the security-enforcing mechanisms have been rightly implemented (i.e., they do exactly what they are intended to do, such as performing some calculation). Effectiveness denotes assurance that the security-enforcing mechanisms of the system meet the stated security objectives (i.e., they do not do anything other than what is intended for them to do, while satisfying expectations for resiliency).

(2). *Leading versus Lagging Indicators:* Leading and lagging indicators reflect security conditions that exist respectively before or after a shift in security. A lagging security metric with a short latency period or lag time is preferred over one with a long latency period. Many security metrics can be viewed as lagging indicators

(3). *Organizational Security Objectives Organizations exist for different purposes*, hold different assets, have different exposure to the public, face different threats, and have different tolerances to risk. Because of these and other differences, their security objectives can vary significantly. Security metrics are generally used to determine how well an organization is meeting its security objectives.

(4). *Qualitative and Quantitative Properties:* Qualitative assignments can be used to represent quantitative measures of security properties (e.g., low means no vulnerabilities found; medium, between one and five found; and high, more than five found). Quantitative valuations of several security properties may also be weighted and combined to derive a composite value.

(5). *Measurements of the Large Versus the Small:* Security measurements have proven to be much more successful when the target of assessment is small and simple rather than large and complex. As the number of components in a system increases, the number of possible interactions increases with the square of the number of components. Greater complexity and functionality typically relate inversely to security and require more scrutiny to evaluate.

3.9. The Value of Security Metrics

Metrics can be an effective tool for security managers to discern the effectiveness of various components of their security programs, the security of a specific system, product or process, and the ability of staff or departments within an organization to address security issues for which they are responsible. Metrics can also help identify the level of risk in not taking a given action, and in that way provide guidance in prioritizing corrective actions. Additionally, they may be used

to raise the level of security awareness within the organization. Finally, with knowledge gained through metrics, security managers can better answer hard questions from their executives and others, such as [1]:

- Are we more secure today than we were before?
- How do we compare to others in this regard?
- Are we secured enough?

Metrics can be an effective tool for security managers to discern the effectiveness of various components of their security programs, the security of a specific system, product or process, and the ability of staff or departments within an organization to address security issues for which they are responsible. Metrics can also help identify the level of risk in not taking a given action, and in that way provide guidance in prioritizing corrective actions. Additionally, they may be used to raise the level of security awareness within the organization [1].

4. Information Security Metrics' Advantages

The use of security metrics could bring a great number of organizational and financial advantages for the organization. It could improve the sense of responsibility with regard to the organizations' information security. Through the results obtained, organizations' management can locate the technical, operational, or managerial measures which are correctly or incorrectly implemented. These results make it possible to locate the problems and solve them. In this way, security metrics could be a useful lever to release the necessary funds for the information security functions. In addition the use of security metrics makes it possible to check and attest that the activities of the organization are in agreement with the applicable laws (compliance concept) [21].

5. Security Metrics Classification According to Performance

The security metrics measuring the performance can be classified in two groups [21]:

(1). *Security metrics related to the effectiveness*: To evaluate to what degree the objectives are being met;

(2). *Security metrics related to the efficiency*: Which shows the proportionality between the objectives being reached and the results being obtained. The use of security metrics confirms that the organization applies a proactive fail-safe attitude. These security metrics inform on the effectiveness of the processes, procedures and controls implemented into the organization.

6. Diverse Classifications of Security Metrics

6.1. The CIS, Center for Internet Security

The CIS, Center for Internet Security [6, 23], has defined a set of security metrics that can be grouped in management metrics, operational metrics or technical metrics based on their purpose and audience, as shown in table (1) [6].

Table 1. *The CIS Security Metrics [6].*

Category	Scope
Management metrics	Provide information on the performance of business functions, and the impact on the organization Audience: Business management
Operational metrics	Used to understand and optimize the activities of business functions Audience: Security management
Technical metrics	Provide technical details as well as a foundation for other metrics Audience: Security operations

6.2. Metrics in the View of Business Imperatives for Information Security

After analyzing the determinants of the business imperatives for information security, Gary Hinson and Krag Brotby [6, 24] have made a kind of update to the list in the previous paragraph. The determinants are the organization's purpose, objectives, business strategies, risks and opportunities and what the organization wants to achieve through information security. This will lead to the definition of the security metric that are needed. For the sake of that selection, metrics have been grouped in three categories, as shown in table (2) [6]:

Table 2. *Types of Security Metrics [6].*

Name	Description
Strategic security metrics	Measures concerning the information security elements of high level business goals, objectives and strategies.
Security management metrics	Metrics that directly relate to achieving specific business objectives for information security
Operational security metrics	Metrics of direct concern to people managing and performing security activities: technical and nontechnical security metrics updated on a weekly, daily or hourly basis.

6.3. Metrics Supporting Control Objectives

The information security business has designed many security frameworks that are internationally used. Among the most popular are the Control Objectives for Information Technology (COBIT), the ISO 27000 series of standards, specifically designed for information security matters and the Information Technology Infrastructure Library (ITIL). Professionals also often refer to the set of documents about information security that the United States National Institute of Standards and Technology (US NIST) publish under the Special Publication 800 Series. Those frameworks enumerate some metrics that are tightly connected to the control objectives of the frameworks. The control objectives covered [6, 25] are:

- information security policy document
- review of the information security policy
- inventory of assets
- ownership of assets

- Acceptable use of assets.

With those various security metrics in hand, IT professionals can rely on scorecard to assist in using the metrics outside the IT room. A scorecard is a statistical record used to measure achievement or progress toward a particular goal. Such tools are very valuable when aligning some function to the business, as is the case of information security. A security scorecard connects the organization's strategies and policies in information security to their potential to improve the core business [6].

The security scorecard is an effective internal communication tool for organizations. Numerous benefits are attached to a security scorecard. Tightening security program to business improves implementation of that program as there is no more discussion about what are the values it adds to the business. The process of request for resources is softened and credibility of the request as well as the one of the program are increased. This goes with increase in accountability: those allocating resources know exactly what they are allocating them for and those in charge of implementation [23] of the program have clear view of what results they accountable for [6].

Establishment of a security metrics program or design of a security scorecard is a matter of appropriate combination of several ingredients that are expected, once mixed together, to produce the unique product that will serve the organization. Most authors, [6, 26], [6, 27] and [6, 24] for example, insist on the starting point being the organization's purpose. The organization's objectives indicate why information security can be relevant to the business executives. And the answer to that question is selecting which metrics have to be present in the security scorecard [6].

7. Applications of Metrics

This section explains the roles and purpose of information security metrics in the overall organizational context [4].

7.1. Security Management Component

In most general terms, within the scope and context of this report, 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 [4, 27, 28], and various other sources on which this report is based.

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 of the major uses of information security metrics from the organizational perspective include [4]:

- Demonstrating compliance or verifying the extent to which security requirements have been satisfied, with regards to both external agents (e.g. laws, regulations, standards, contractual obligations) and internal ones (e.g. organizational policies and procedures).
- Increasing transparency and improving accountability by facilitating detection of specific security controls that are not properly implemented (or not at all) or are otherwise ineffective, and the stakeholders in charge.
- Improving effectiveness and efficiency of security management by providing the means to monitor and gauge the security posture in view of different events and activities, correlate implementation of particular security strategies with changes in posture, display trends, and quantify progress towards objectives.
- Supporting resource allocation related decisions by providing quantitative means to either justify and reflect on the prior/current information security spending or plan and prioritize future investments.
- Enabling quality assurance and assessment of suitability when acquiring security products or services from third parties and providing means to compare different products and services.

7.2. Relationship to Risk Management

Security metrics 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. Therefore, 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 [4].

This relationship is, for instance, highlighted in the ISO/IEC 27004 standard, where it is both explicitly stated that an organization is required to have a sound understanding of the security risks it faces prior to developing metrics and performing measurement, and that the output of measurement can substantiate risk management processes [4, 29]. Thus, the relationship between security measures and risk management is both interdependent and mutually beneficial [4].

8. Conclusions and Recommendations

Security metrics can be considered as a standard (or system) used for quantitatively measuring an organization's security posture. Security metrics are essential to comprehensive network security and CSA management. Without good metrics, analysts cannot answer many security related questions. Measuring information security is difficult. Effective measurement and reporting are required in order to demonstrate compliance, improve effectiveness and efficiency of controls, and ensure strategic alignment in an

objective, reliable, and efficient manner.

We would thus recommend that metrics must be designed using a participatory design process involving the affected security professionals of the organization. Moreover, using a method where the availability of data is prioritized higher than the completeness of the metrics is recommended in order to test and improve the maturity of the information security program.

References

[1] Deepti Juneja, Kavita Arora, Sonia Duggal, "Developing Security Metrics For Information Security Measurement System", International Journal of Enterprise Computing and Business Systems, Vol. 1 Issue 2 July 2011, http://www.ijecbs.com.

[2] Christina Kormos, et al, "Using Security Metrics To Assess Risk Management Capabilities", 1999.

[3] Kristoffer Lundholm, Jonas Hallberg, Helena Granlund, "Design and Use of Information Security Metrics", Report no FOI-R--3189—SE, Application of the ISO/IEC 27004, 2011.

[4] Rostyslav Barabanov, "Information Security Metrics: State of the Art", DSV Report series No 11-007, Mar 25, 2011.

[5] Rainer B¨ohme, "Security Metrics and Security Investment Models", International Computer Science Institute, Berkeley, California, USA, 2010.

[6] Perpétus Houngbo, Joël Hounsou, "Measuring Information Security: Understanding And Selecting Appropriate Metrics", International Journal of Computer Science and Security (IJCSS), Volume (9): Issue (2): 2015.

[7] http://www.oxforddictionaries.com/definition/english/metric.

[8] http://www.oxforddictionaries.com/definition/english/measurement.

[9] http://www.oxforddictionaries.com/definition/english/measure.

[10] A. C. S. Associates, Information System Security Attribute Quantification or Ordering (Commonly but improperly known as “Security Metrics”). 2001.

[11] P. E. Black, K. Scarfone, and M. Souppaya, “Cyber security metrics and measures,” Wiley Handb. Sci. Technol. Homel. Secur., 2008.

[12] V. Verendel, “Quantified security is a weak hypothesis: a critical survey of results and assumptions,” in Proceedings of the 2009 workshop on New security paradigms workshop, 2009, pp. 37–50.

[13] S. C. Payne, “A guide to security metrics,” Inst. Inf. Secur. Read. Room, 2006.

[14] Marte Tarnes, "Information Security Metrics: An Empirical Study of Current Practice", Specialization Project, Trondheim, 17th December 2012.

[15] Shirley C. Payne. A Guide to Security Metrics. SANS Institute Information Security Reading Room, June 2006.

[16] Lance Hayden. IT Security Metrics: A Practical Framework For Measuring Security & Protecting Data. McGraw-Hill Osborne Media, first edition, 2010.

[17] Andrew Jaquith. Security Metrics: Replacing Fear, Uncertainty, and Doubt. Addison-Wesley Professional, first edition, 2007.

[18] ISO/IEC 27004: 2009(E). Information technology - Security techniques - Information security management - Measurement - First edition. International Organization for Standardization, 2009.

[19] Chapin, D. A. & Akridge, S. (2005). How can security be measured? Information Systems Control Journal, http://www.isaca.org/Journal/Past-Issues/2005/Volume-2/Pages/default.aspx (2005). How can security be measured? Information Systems Control Journal, http://www.isaca.org/Journal/Past-Issues/2005/Volume-2/Pages/default.aspx.

[20] Jaquith, A., Security metrics: Replacing fear, uncertainty, and doubt. Upper Saddle River, NJ: Addison-Wesley, 2007.

[21] Igli TASHI, Solange GHERNAOUTI-HÉLIE, "Security metrics to improve information security management", In Proceedings of the 6th Annual Security Conference, April 11-12, 2007, Las Vegas, NV, www.security-conference.org.

[22] D. Hubbard, Measure for measure: The Actuary, official magazine of SIAS and The Actuarial Profession, 2014.

[23] T. C. for I. Security, The CIS Security Metrics, 2010.

[24] M. Hoehl, Creating a monthly Information Security Scorecard for CIO and CFO. SANS Institute, 2010.

[25] J. Breier and L. Hudec, “Risk analysis supported by information security metrics,” in Proceedings of the 12th International Conference on Computer Systems and Technologies, pp. 393–398, 2011.

[26] S. C. Payne, “A guide to security metrics,” Inst. Inf. Secur. Read. Room, 2006.

[27] ISO/IEC (2009a). ISO/IEC 27004: 2009, Information technology -- Security techniques -- Information security management -- Measurement. Geneva: ISO.

[28] Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2008). Performance measurement guide for information security. Gaithersburg, MD: National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

[29] ISO/IEC (2009a). ISO/IEC 27004: 2009, Information technology -- Security techniques -- Information security management -- Measurement. Geneva: ISO.