Security Metrics and the Risks: An Overview

Rana Khudhair Abbas Ahmed

AlRafadian University College/ Computer Techniques Engineering Department

Baghdad, Iraq

Abstract— *measuring information security is difficult; it is difficult to have one metrics that covers all types of devices. Security metrics is a standard used for measuring any organization's security. Good metrics are needed for analysts to answer many security related questions. Effective measurement and reporting are required to improve effectiveness and efficiency of controls, and ensure strategic alignment in an objective, reliable, and efficient manner. This paper provides an overview of the security metrics and its definition, standards, advantages, types, problems, taxonomies, risk assessment methods and also classifies the security metrics and explains its risks.*

Keywords— *Security, Metrics, advantages, Problems, Risk management.*

I. 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].

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].

II. 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**.**

III. INFORMATION SECURITY METRICS' CONCEPT

A. 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].

B. 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].

C. Determining Attributes of a Good Information Security Metric [19]

A good metric should meet the following attributes:

1) It must be consistently measured, without subjective criteria.
2) It must be cheap to gather, preferably in an automated way.
3) It must be expressed as a cardinal number or percentage, not with qualitative labels like “high,” “medium,” and “low”.

It must be expressed using at least one unit of measure, such as “defects,” “hours,” or “dollars”.

D. 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.) [20].

IV. SECURITY METRICS STANDARDS'

We have prepared table (I) to define security metrics standards.

TABLE I: SECURITY METRICS STANDARDS.

Security Metrics Standards	Definition
ISO27002	Was a development of the ISO17799 standard. It contains controls that can be implemented based on ISO27001. The ISO27001 is a specification for an Information Security Management System. These two documents are meant to be used together.
ISO27004	This standard is still under development. It attempts to overcome some of the criticism that has been leveled at ISO27002. This includes, but is not limited to, the following i.e. it being a risk assessment tool as opposed to a benchmark, the lack of clarity with definitions etc.
IS1 (Information Security Standard 1)	The UK Government’s Information Security Standard 1 is a stringent risk assessment methodology that was developed to meet the requirements of the UK Government. It replaces the existing HMG Infosec Standard No. 1 and the HMG Infosec Standard No. 3.
USA NIST (National Institute of Standards and Technology)	In 2003, the NIST came up with a Guide for Information Security Metrics. The NIST metrics is designed for US federal government use but its standards can be applied to other organizations with differing environments. It is similar to the UK government provisions for data security and assurance.

V. Similarity between Metrics

Most security metrics advocate some type of lifecycle which starts by establishing objectives, performing risk assessments and ends by implementing controls. Before a risk assessment can be undertaken however, the goals of the exercise have to be determined – is the audit going to be based on an organization's goals and objectives or is a framework (like the ISO27002) going to be used as a baseline. Establishing goals ensures that the risk is assessed in view of agreed objectives. Most metrics systems then advocate a risk assessment. This involves undertaking an audit to assess the risk present. The results are then used to determine which sets of controls need to be implemented. There are various risk assessment methodologies. We look at some in the next section. They commonly involve some method of specifying the source of data, frequency of data collection, which is responsible for the accuracy of the data, and the compilation of data for measurement purposes. There are various views on the methods of assessing risk and there are just as many criticisms on the formal methods. This should be kept in mind when performing an assessment [21].

IV. 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) [22].

VII. The Problems with Metrics

Most standards are implemented from an auditor's perspective. ISO27002 and the IS1 are cases-in-point. They do not provide any help in measuring or monitoring the effectiveness of controls. Instead they measure the existence of controls. This is what led to the development of ISO27004. The independent nature of standards also means that if you use a metric as a framework, your security controls are not going to align with business standards. Standards tend to be general as opposed to meeting the goals of different industries. The process of ensuring that your security controls support your business goals and objectives, and do not hinder them, tends to make the exercise of measuring the effectiveness of controls more difficult and time consuming. However the end result will far more accurately reflect the real effectiveness of the security implementation. It is impossible to list all the controls in a general purpose standard and thereby give advice tailored to the needs of specific industries [21].

Different industries have a range of workplace challenges as the work is conducted in differing environments. They are also subject to different regulations. The medical and financial industry would normally have much more stringent regulations imposed on them then the retail sector. Another issue to contend with is the installed base of a piece of software. Due to a larger installation base with for e.g. Microsoft, its vulnerabilities appear to be more prevalent as hackers tend to target that which is readily available. Customized software might have virtually no published vulnerabilities but might in fact have more threats if security was not considered during development. Security is often reduced to the pure fulfilment of a standard. This diminishes the value of the standard. The trouble is that an auditor highlights non-compliance as a finding. Non familiarity with the industry is why the auditor cannot make a call either way. This tends to happen with most with technical controls. Management is usually reluctant to strike the finding off and the goal is to comply with the standard and everything and anything towards that goal is acted upon. As such, processes that might not be required or that result in a waste of time might get put into place without much thought to how they ensure compliance. It is just easier that way [21].

VIII. The Challenges with Building Metrics

One of the big challenges of building a metric is the scope that has to be considered. There are a wide range of threats to security which are non-technical, for example natural disasters. Additionally there are many layers to security for example technical security has network security, application security etc. As such there are a lot of variables to contend with. To just list and document each might be an exercise in futility. It can be difficult to quantify security controls. It is difficult to do an apple-to-apple comparison as controls can be implemented differently, yet have the same goal. In this type of case, what values can you use to determine which one is better? There is also the issue of one metric versus a suite of metrics. It is highly unlikely that a single metric will reflect accurately how effectively security was implemented [21].

There are a large number of platforms in use which may implement controls differently. There are a large number of environments in which these controls will operate in. And these environments have different threats. They operate under differing regulations. Security is the responsibility of all parties. The manufacturer cannot build security into

their product and then make a claim as to it being a 100% secure. The user also has a responsibility. Security currently tends to be looked at from the viewpoint of the manufacturer. The user's responsibility to behave responsibly needs to be taken into consideration as well. What can and cannot be measured has to be defined. Some things can be hard to measure. We need to be able to effectively measure human capabilities and awareness? We need to quantify human capabilities. These play a vital part in security as well. Sometimes it is the most important part [21].

XI. 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 [23]:

- Governance, Management, and Technical.
- Management, Operational, and Technical.
- Organizational, Operational, and Technical.
- (Information Assurance) Programme Development, Support, Operational, and Effectiveness.
- Organizational and Performance, Operational, Technological, Business Process, Business Value, and Compliance.
- Implementation, Effectiveness and Efficiency, and Business Impact.
- In (CIS, 2009), though not explicitly stated, proposed metrics can potentially be categorized by their target audience, which is Management, Operations.

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 [23].

XII. Diverse Classifications of Security Metrics

A. The CIS, Center for Internet Security:

The CIS, Center for Internet Security [6, 24], 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 II [6].

TABLE II: 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

B. Metrics in the view of business imperatives for information security:

After analysing the determinants of the business imperatives for information security, Gary Hinson and Krag Brotby [6, 25] 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 III [6]

TABLE III: 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

C. 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, 26] 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 [24] 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, 27], [6, 28] and [6, 25] 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].

XIII. RISK ASSESSMENT METHODOLOGIES

The purpose of performing a risk assessment is to ensure that the security controls (when implemented) fully commensurate with the risks. The process helps provide hard facts to back up any security problems that might crop up. It helps to prioritize which controls to implement [21]. We have prepared table IV to explain different risk assessment methods with their results.

TABLE IV: DIFFERENT RISK ASSESSMENT METHODS WITH THEIR RESULTS.

Risk Assessment Methods	Results
Failure Mode and Effects Analysis	Examines each potential failure condition in a system to determine the severity of the impact to the system.
Hazard and Operability (HAZOP)	Examines process and engineering intentions to assess the potential hazards that can arise from deviations from design specifications.
Historical Analysis	Examines frequency of past incidents to determine the probability of a condition recurring
Human-Error Analysis	Examines the possible impact of human intervention and error on a system.
Probabilistic Risk Assessment	Examines the probability that a combination of events will lead to a particular condition.
Tree Analysis	Is a family of methods that focus on processes or a sequence of events that may lead to a particular condition.

XIV. APPLICATIONS OF METRICS

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

A. Security Management Component

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, 28, 29].

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

B. 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, 30]. Thus, the relationship between security measures and risk management is both interdependent and mutually beneficial [4].

XV. CONCLUSIONS AND RECOMMENDATIONS

Metrics are important to information security because metrics can be an effective tool for information security professionals to measure the security strength and levels of their systems, products, processes, and readiness to address security issues they are facing. There is little that makes one security method stand out among the others. Most of these approaches to risk assessment tend to be incomplete. They fail to include all components of risk.

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] Scott E. Schimkowitsch, et al., " Key Components of an Information Security Metrics Program Plan", capstone report, University of Origon, 2009.

[20] 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

[21] Manwinder Kaur, Andy Jones, " Security Metrics - A Critical Analysis of Current Methods", Proceedings of the 9th Australian Information Warfare and Security Conference, Symposia and Campus Events, 2008.

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

[23] Rostyslav Barabanov, "Information Security Metrics: Research Directions", Stockholm Stewart Kowalski Stockholm, 2011.

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

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

[26] 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.

[27] S. C. Payne, "A guide to security metrics," Inst. Inf. Secur. Read. Room, 2006.

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

[29] 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

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