International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(4): 280-288
The Society of Digital Information and Wireless Communications (SDIWC), 2012 (ISSN: 2305-0012)

Technical Security Metrics Model in Compliance with ISO/IEC 27001 Standard

M.P. Azuwa, Rabiah Ahmad, Shahrin Sahib and Solahuddin Shamsuddin
azuwa70@student.utem.edu.my, {rabiah,shahrin}@utem.edu.my
solahuddin@cybersecurity.my

ABSTRACT

Technical security metrics provide measurements in ensuring the effectiveness of technical security controls or technology devices/objects that are used in protecting the information systems. However, lack of understanding and method to develop the technical security metrics may lead to unachievable security control objectives and inefficient implementation. This paper proposes a model of technical security metrics to measure the effectiveness of network security management. The measurement is based on the security performance for (1) network security controls such as firewall, Intrusion Detection Prevention System (IDPS), switch, wireless access point and network architecture; and (2) network services such as Hypertext Transfer Protocol Secure (HTTPS) and virtual private network (VPN). The methodology used is Plan-Do-Check-Act process model. The proposed technical security metrics provide guidance for organizations in complying with requirements of ISO/IEC 27001 Information Security Management System (ISMS) standard. The proposed model should also be able to provide a comprehensive measurement and guide to use ISO/IEC 27004 ISMS Measurement standard.

KEYWORDS

Information security metrics, technical security metrics model, measurement, vulnerability assessment, ISO/IEC 27001:2005, ISO/IEC 27004:2009, Critical National Information Infrastructure.

1 INTRODUCTION

The phenomena of instant grow and increasing number of cyber attacks has urged the organizations to adopt security standards and guidelines. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) has developed the ISO/IEC 27000 series of standards that have been specifically reserved for information security matters. Through ISO/IEC 27001 Information Security Management System (ISMS) – Requirements [1], the organization may comply and obtain the certification in increasing level of protection for their information and information systems.

Information security metrics can be ineffective tools if organizations do not have data to measure, procedures or processes to follow, indicators to make good protection decisions and people to develop and report to the management.

To be useful, measurement of information security effectiveness should be comparable. Comparisons are usually made on the basis of quantifiable measurement of a common characteristic. The main problems in the information security metrics development are identified; (i) lack of clarity on defining quantitative effective security metrics to the security standards and guidelines; (ii) lack of method to guide the organizations in choosing security objectives, metrics and

measurements for mitigating current cyber attacks [2][3].

Hulitt and Vaughn [4] report, lack of clarity in a standard quantitative metric to describe information system's level of compliance with the FISMA standard, even though thorough and repeatable compliance assessment conducted using Risk Management Framework (RMF). Bellovin [5] remarks that defining metrics is hard. It is not infeasible, because an attacker's effort is often linear, even when the exponential security work is needed. Those pursuing the development of a security metrics program should think of themselves as pioneers and be prepared to adjust strategies as experience dictate [6]. It is also known that ISO/IEC 27001 provides generic guidance in developing the security objectives and metrics and still lack of method to guide the organizations [2][3].

1.1 Information Security Metrics

In understanding the meaning of information security metrics, the security practitioners and researchers have simplified their definitions of information security metrics and measures (as described in Table 1).

Table 1: Definitions of Information Security Metrics and Measures

Author	Definition
Stoddard et al. [7]	A metric is a measurement that is compared to a scale or benchmark to produce a meaningful result. Metrics are a key component of risk management.
Savola [8]	Security Metric is a quantitative and objective basis for security assurance. It eases in making business and engineering decisions concerning information security. The metrics are derived from comparing two or more measurements taken over time with a predetermined baseline.
Brotby [9]	The *metric* is a term used to denote a measure based on a reference and involves at least two points, the measure and the reference. A *security* is the protection from or absence of danger. The security metrics are categorized by what they measure. The measures include the process, performance, outcomes, quality, trends, conformance to standards and probabilities.
Masera et al. [10]	"Security metrics are indicators, and not measurements of security. Security metrics highly depend on the point of reference taken for the measurement, and shouldn't be considered as absolute values with respect to an external scale."
Hallberg et al. [11]	"A security metric contains three main parts: a *magnitude, a scale and an interpretation*. The security values of systems are measured according to a specified magnitude and related to a scale. The interpretation prescribes the meaning of obtained security values."
Lundholm et al. [12]	The measurement quantifies only a single dimension of the object of measurement that does not hold value (facilitate decision making) in itself. The metric is derived from two or more of the measurement to demonstrate an important correlation that can aid a decision.

From these definitions, we propose the definition as information security metrics is a measurement standard for information security controls that can be quantified and reviewed to meet the security objectives. It facilitates the relevant actions for improvement, provide decision making and guide

compliancy to security standards. Information security measurement is a process of measuring/assessing the effectiveness of information security controls that can be described by the relevant measurement methods to quantify data and the measurement results are comparable and reproducible. Hence, information security measurement is a subset of information security metric.

1.2 Technical Security Metrics and Measurement

We found the research activities for technical security metrics are very limited. Also, there is lack of specific technical security metrics research to measure the technical security controls from a total 133 security controls from the ISO/IEC 27001 standard.
Vaughn et al. [13] define *Technical Target of Assessment (TTOA)* as to measure how much a technical object, system or product is capable of providing assurance in terms of protection, detection and response. According to Stoddard et al. [7], technical security metrics are used to assess technical objects, particularly products or systems [8], against standards; to compare such objects; or to assess the risks inherent in such objects.
Additionally, the technical security metrics should be able to evaluate the strength in resistance and response to attacks and weaknesses (in terms of threats, vulnerabilities, risks, anticipation of losses in face of attack) [13]. At the same time, it indicates the security readiness with respect to a possible set of attack scenarios [10].

1.3 Effective Measurement Requirement from ISO/IEC 27001 Standard

Information security measurement is a mandatory requirement in ISO/IEC 27001 standard where it is indicated in a few clauses in: 4.2.2(d) “Define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results”, 4.2.3(c) “Measure the effectiveness of controls to verify that security requirements have been met”, 4.3.1(g) “documented procedures needed by the organization to ensure the effective planning, operation and control of its information security processes and describe how to measure the effectiveness of controls”, 7.2(f) “results from effectiveness measurements” and 7.3(e) “Improvement to how the effectiveness of controls is being measured”. The importance of information security measurement is well defined in these clauses.

2 SECURITY METRICS DEVELOPMENT APPROACH

The development of technical security metrics model (TSMM) is derived from the following approach:

(1) The requirements of technical security controls are based on ISO/IEC 27002 ISMS – Code of Practices standard [14].
(2) Identify relevant security requirements
(3) Achieve security performance objectives
(4) Align to risk assessment value

(5) The development of technical security metrics should not be an extensive list, but more focus on the critical security controls that provide high impact to the organizations. According to Lennon [15], "the metrics must be prioritized to ensure that the final set selected for initial implementation facilitates improvement of high priority security control implementation. Based on current priorities, no more than 10 to 20 metrics at a time should be used. This ensures that an IT security metrics program will be manageable."
(6) Align to risk assessment value
(7) Ease of measurement.
(8) Provide the process to obtain data/evidence, method and formula to assess the security measurement
(9) Resistance and response to known and unknown attacks
(10) Provide the threshold values to determine the level of protection
(11) Provide actions to improve
(12) Comply to the ISO/IEC 27001 standard

3 TECHNICAL SECURITY METRICS MODEL (TSMM)

The development of TSMM is based on Plan-Do-Check-Act (PDCA) model. The development of TSMM is described in Figure 1.

3.1 PLAN Phase: (Selection of Controls and Definition)

The focus is on the technical security controls that will be extracted from the total 133 security controls as stated in the Annex A of ISO/IEC 27001 standard.

We define technical security metrics as a measurement standard to address the performance of security countermeasures within the technical security controls and to fulfill the security requirements. The technical security measures are based on information security performance objectives that can be accomplished by quantifying the implementation, efficiency, and effectiveness of security controls.

ISO/IEC 27002 [14] provides the best practice guidance in initiating, implementing or maintaining the security control in the ISMS. This standard regards that "not all of the controls and guidance in this code of practice may be applicable and additional controls and guidelines not included in this standard may be required".

Federal Information Processing Standards 200 (FIPS 200) [16] defines technical controls as "the security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system". These are the basis of our definition for technical security controls.

Based on NIST SP800-53 guidelines [17], the technical security controls comprise of:

(1) Access Control (AC-19 controls)
(2) Audit and Accountability (AU-14 controls)
(3) Identification and Authentication (IA-8 controls)
(4) System and Communications Protection (SC-34 controls)

The total of technical security controls from NIST SP800-53 guidelines is seventy-five (75). In the Appendix H of [18], the technical security controls are extracted from Table H-2. This table is mapping from the security controls in ISO/IEC 27001 (Annex A) to NIST Special Publication 800-53. We extract and analyze these technical security controls. We discover that:

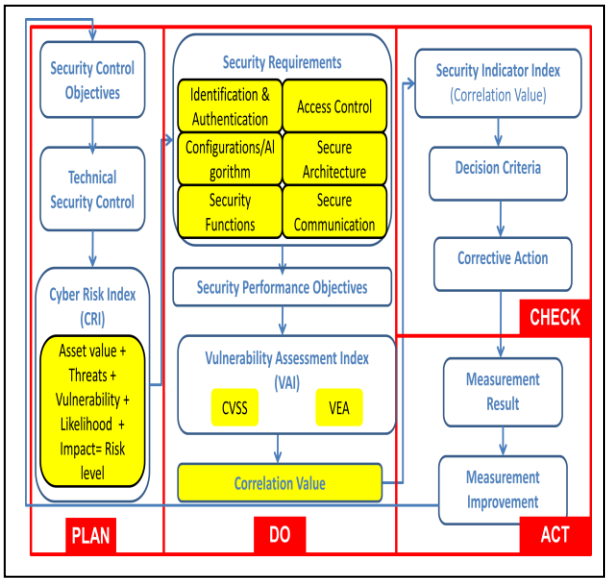
(1) Within three (3) main domains from ISO/IEC 27001 (Annex A) that include:
- A.10 Communications and operations management
- A.11 Access Control
- A.12 Information systems acquisition, development and maintenance

(2) The initial total of technical security controls is forty-five (45).

(3) The identified technical security controls only require a process or policy implementation and not related to technical implementation, such as A.11.1.1 Access control policy, A.11.4.1 Policy on use of network services, A.11.5.1 Secure log-on procedures, A.11.6.2 Sensitive system isolation, A.11.7.2 Teleworking, A.12.3.1 Policy on the use of cryptographic control and A.12.6.1 Control of technical vulnerabilities.

(4) There are relationships with other security controls in NIST SP800-53 document, including:
- Management controls: Security Assessment and Authorization (CA), Planning (PL), System and Services Acquisition (SA)
- Operational controls: Configuration Management (CM), Maintenance (MA), Media Protection (MP), Physical and Environmental Protection (PE), Personnel Security (PS), System and Information Integrity (SI).

Figure 1: Technical Security Metrics Model (TSMM)



The technical security controls should be practical, customized and measured according to organization's business requirements and environments.

A risk management approach will be used in identifying the relevant security controls. Threat and vulnerability assessment will be carried out.

Threat and vulnerability assessment will be carried out. Also, identifying both impact and risk exposure to determine the prioritization of security controls.

Cyber-Risk Index: A cyber-risk index is used to evaluate the vulnerability and threat probabilities related to the successfulness of current and future attacks. Attack-Vulnerability-Damage

(AVD) model [19] and Common Vulnerability Scoring System (CVSS) - Base Metric [20] are used to determine this weighted-index. We will extent and include the criticality or impact of loss to the organization. The CVSS base score is calculated using the information provided by the U.S. National Vulnerability Database (NVD) Common Vulnerability Scoring System Support v2 [21] and other relevant Cyber Emergency Response Team (CERT) Advisories and Report.

3.2 DO Phase: (Effective Measurement)

The security requirements describe the actual security functional for technical security controls in protecting the information systems. Security functional includes the identification and authentication, access control, configurations/algorithm, architecture and communication.

A set of performance objectives is developed for each security requirement. Vulnerability Assessment (VA) Index: The VA index is that can be derived by conducting the security or vulnerability assessment to the information systems through a simulation assessment, vulnerability scanning or penetration testing. This is based on the current assessment of potential attacks and will be weighted-index using the numeric CVSS scores: "Low" severity (CVSS base score of 0.0-3.9), "Medium" severity (CVSS score of 4.0-6.9) and "High" severity (CVSS base score of 7.0-10.0). The VAI can also be derived from Vulnerability-Exploits-Attack (VEAbility) metrics [22]. The VEAbility measures the security of a network that is influenced by the severity of existing vulnerabilities, distribution of services, connectivity of hosts, and possible attack paths. These factors are modeled into three network dimensions: Vulnerability, Exploitability, and Attackability. The overall VEA-bility score, a numeric value in the range [0,10], is a function of these three dimensions.

At this phase, the data collection must be easily obtainable and the measurements are not complicated. The measurement should be able to cater for current (through audit report and evidence of events) and future attacks.

3.3 CHECK Phase: (Security Indicators and Corrective Action)

In verifying the effectiveness of controls, we measure how much the control decreases the probability of realization of the described risks. The attributes must be significant in determining the increase or decrease of risk. The expected measure function can be derived by the percentage of the successful or failure occurrences. For example, number of patches successfully installed on information systems (> 95%), number of security incidents caused by attacks from the network (< 3%). The determination of the percentage should consider that even though the security controls are implemented, the risk of attacks can still occur. Therefore, the percentage depicts the strength of the existing security controls in mitigating the risks.

Security Indicator Index: If the measure is equal to or below the recommendation, the risk is adequately controlled, thus explain the effectiveness of the security controls. The proposed indicators are the trends of the derived measures and they must be within the

same measurement scale in order to establish that the risk is adequately controlled [23]. This indicator index can also act as a compliance index to ISO/IEC 27001 standard. Algorithm or calculation combining one or more base and/or derived measures with associated decision criteria. For example: 0-60% - Red; 60-90% - Yellow; 90-100% Green.

Decision Criteria: Thresholds, targets, or patterns used to determine the need for action or further investigation, or to describe the level of confidence in a given result (for example, Red – intervention is required, causation analysis must be conducted to determine reasons for non-compliance and poor performance; Yellow – indicator should be watched closely for possible slippage to Red; Green – no action is required).

Corrective actions provide the range of Potential changes in improving the efficiency and effectiveness of the security controls. They can be prioritized based on overall risk mitigation goals and select based on cost-benefit analysis.

3.4 ACT Phase:

The developed technical security metric and measurement will be validated by the respective organizations. The metric is to comply to ISO/IEC 27001 standard requirements. The development of technical security metrics will be based on Information security measurement model in ISO/IEC 27004 standard.

The measurement result should be reported to the management in ensuring the continuity and improvement of information security in the organization.

4 CONCLUSIONS AND FUTURE WORK

Malaysia government has seen the importance of Critical National Information Infrastructure (CNII) organizations to protect their critical information systems. In the year of 2010, the government has mandated for their systems to be ISO/IEC 27001 ISMS certified within 3 years [24].

The ISO 27001 certification is one of the most used corporate best practices for IT security standards, addressing management requirements as well as identifying specific control areas for information security. It provides a comprehensive framework for designing and implementing a risk-based Information Security Management System. The requirements and guidance cover policies and actions that are necessary across the whole range of information security vulnerabilities and threats. By customizing the security requirements from ISO/IEC 27002 and other relevant security standards and guidelines, the CNII organizations will implement the necessary security controls in compliance with ISO/IEC 27001 ISMS standard.

The proposed TSMM is to provide guidance for CNII organizations to measure the effectiveness of the network security controls in compliance with ISO/IEC 27001 standard. The relevant type of information security measurement and metrics are interrelated and worth to use in aligning with business risk management. We also want to explore the usability of the ISO/IEC 27004 standard and conduct a case study at several CNII organizations.

ACKNOWLEDGMENT

The authors wish to acknowledge and thank members of the research teams of the Long Term Fundamental Research Grant Scheme (LRGS) number LRGS/TD/2011/UKM/ICT/02/03 for this work. The research scheme is supported by the Ministry of Higher Education (MOHE) under the Malaysian R&D National Funding Agency Programme.

5 REFERENCES

1. International Organization for Standardization and International Electrotechnical Commission, "Information technology - Security techniques - Information security management systems-Requirements," *ISO/IEC 27001:2005*, 2005.
2. R. Barabanov, S. Kowalski, and L. Yngström, "Information Security Metrics: Research Directions," *FOI Swedish Defence Research Agency*, 2011.
3. C. Fruehwirth, S. Biffl, M. Tabatabai, and E. Weippl, "Addressing misalignment between information security metrics and business-driven security objectives," *Proceedings of the 6th International Workshop on Security Measurements and Metrics - MetriSec '10*, p. 1, 2010.
4. E. Hulitt and R. B. Vaughn, "Information system security compliance to FISMA standard: A quantitative measure," *2008 International Multiconference on Computer Science and Information Technology*, no. 4, pp. 799–806, Oct. 2008.
5. S. M. Bellovin, "On the Brittleness of Software and the Infeasibility of Security Metrics," *IEEE Security & Privacy Magazine*, vol. 4, no. 4, pp. 96–96, Jul. 2006.
6. K. Stouffer, J. Falco, and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security," *National Institute of Standards and Technology, NIST Special Publication 800-82*, no. June, 2011.
7. J. Stoddard, M., Bodeau, D., Carlson, R., Glantz, C., Haimes, Y., Lian, C., Santos, J., and Shaw, "Process Control System Security Metrics – State of Practice," *Institute for Information Infrastructure Protection (I3P)*, vol. Research R, no. August, 2005.
8. R. Savola, "Towards a Security Metrics Taxonomy for the Information and Communication Technology Industry," in *International Conference on Software Engineering Advances*, 2007.
9. W. K. Brotby, *Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement*. Auerbach Publications, 2009.
10. M. Masera and I. N. Fovino, "Security metrics for cyber security assessment and testing," *Joint Research Centre of the European Commission,*, vol. ESCORTS D4, no. August, pp. 1–26, 2010.
11. J. Hallberg, M. Eriksson, H. Granlund, S. Kowalski, K. Lundholm, Y. Monfelt, S. Pilemalm, T. Wätterstam, and L. Yngström, "Controlled Information Security: Results and conclusions from the research project," *FOI Swedish Defence Research Agency*, pp. 1–42, 2011.
12. H. Lundholm, K., Hallberg, J., Granlund, "Design and Use of Information Security Metrics," *FOI, Swedish Defence Research Agency*, pp. ISSN 1650–1942, 2011.
13. J. Rayford B. Vaughn, R. Henning, and A. Siraj, "Information Assurance Measures and Metrics - State of Practice and Proposed Taxonomy," in *Proceedings of the 36th Hawaii International Conference on System Sciences*, 2003, p. 10 pp.
14. International Organization for Standardization and International Electrotechnical Commission, "Information technology - security techniques - Code of practice for information security management," *ISO/IEC 27002:2005*, vol. 2005, 2005.
15. E. B. Lennon, M. Swanson, J. Sabato, J. Hash, L. Graffo, and N. Sp, "IT Security Metrics," *ITL Bulletin, National Institute of Standards and Technology*, no. August, 2003.
16. W. J. Carlos M. Gutierrez, "Federal Information Processing Standards 200 - Minimum Security Requirements for Federal Information and Information Systems," *National Institute of Standards and Technology,*, no. March, 2006.
17. Computer Security Division and Information Technology Laboratory, "Recommended Security Controls for Federal Information Systems and Organizations," *National*

Institute of Standards and Technology, NIST Special Publication 800-53 , Revision 3, 2010.

18. Computer Security Division and I. T. Laboratory, "Security and Privacy Controls for Federal Information Systems and Organizations," *National Institute of Standards and Technology, NIST Special Publication 800-53 , Revision 4*, no. February, 2012.
19. T. Fleury, H. Khurana, and V. Welch, "Towards A Taxonomy Of Attacks Against Energy Control Systems," in *Proceedings of the IFIP International Conference on Critical Infrastructure Protection*, 2008.
20. P. Mell, K. Scarfone, and S. Romanosky, "A Complete Guide to the Common Vulnerability Scoring System," *Forum of Incident Response and Security Teams, FIRST Organization*, pp. 1–23, 2007.
21. "NVD Common Vulnerability Scoring System Support v2," *NIST, National Vulnerability Database (NVD), http://nvd.nist.gov/cvss.cfm?version=2*.
22. M. Tupper and a. N. Zincir-Heywood, "VEA-bility Security Metric: A Network Security Analysis Tool," *2008 Third International Conference on Availability, Reliability and Security*, pp. 950–957, Mar. 2008.
23. M. H. S. Peláez, "Measuring effectiveness in Information Security Controls," *SANS Institute InfoSec Reading Room, http://www.sans.org/reading_room/whitepapers/basics/measuring-effectiveness-information-security-controls_33398*, 2010.
24. J. P. M. Malaysia, "Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam," *Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU)*, vol. MAMPU.BPIC, p. 1, 2010.