IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITP4667

Measuring Information Security: Combining the SSE-CMM with the ISO 17799 Standard

Vaughn Christie and James Goldman
Department of Computer Technology, Purdue University
vrchristie@tech.purdue.edu, jegoldman@tech.purdue.edu
(Christie) 765-495-1312, (Goldman) 765-494-9525

ABSTRACT

Information security (IS) incidents are on the rise with new attacks reported daily. How have system administrators and security professionals reacted to these new threats? Traditionally, system owners have rushed to "acquire the latest cure" (Nielsen, 2000). They have implemented today's fix with little thought to the benefit truly gained from such tools. This historical approach to system security is yielding to a model of increased accountability. In short, IS professionals are being asked, "How secure are we?" (Payne, 2001).

Answers to this and similar questions are not easily derived (Payne, 2001). Dating back to the late 1970's and early 1980's, when the annual loss expectancy (ALE) calculation was being developed, security professionals have attempted to define security by a single distinct value: ALE (Fletcher, 1995). Since that time, additional IS management documents, defined by Fletcher (1995) as third-generation information security tools, have been developed, including a number of guidance documents, which have been published to assist organizations in establishing and maintaining their IT security programs. Examples include the NIST Handbook, the CSE Guide, ISO 17799, etc. (Hopkins, 1999). Unfortunately, problems reside in these guidance tools; specifically, they lack the ability to measure defined IS parameters easily, effectively or efficiently (Payne, 2001).

This research has yielded a metric-based IS maturity framework constructed from the combination of the ISO 17799 standard and the Systems Security Engineering Capability Maturity Model (SSE-CMM). The study has illustrated the complementary nature of the SSE-CMM and ISO standard and shown how the SSE-CMM can be leveraged to assess the maturity of the practices implemented according to ISO 17799 standard specifications. The end result is a self-facilitated metrics-based security assessment (MBSA) framework, which will allow organizations to assess the maturity of their IS processes. By using the SSE-CMM to measure the maturity of industry accepted IS process standards, the findings of this study enable professionals to measure, in a more consistent, reliable, and timely manner, areas for improvement and effectiveness. Furthermore, the findings allow a more dependable qualitative measurement of the returns achieved through given IS investments. Ultimately, this research has provided professionals an additional, more robust self-assessment tool in answering: "How secure are we?"

THE PROBLEM

Sparked by a combination of 9/11, the mounting complexity of online attacks, and the increasing realization that network surveillance, intrusion detection and real-time response strategies are organizational responsibilities, IS has come to the forefront of organizational agendas (Dargan, 2002). However, even with mounting media attention and increases in IT spending, data reported by Ultima Business Solutions suggests that IT teams are increasingly failing to protect organizations from attack (Dargan, 2002).

As such, IT security projects are coming under greater scrutiny, and IS managers are increasingly being asked to demonstrate a return on the investments being made. In brief, (Payne, 2001):

- "Are we more secure today than we were before?"
- "If so, how do we know?"
- "How do we compare to our competition?"
- "How secure are we?"

How will these questions be answered? In recent years, guidance documents have evolved that have attempted to qualitatively guide corporations in addressing these questions (Hopkins, 1999). While each differs from its peers, in structure, culture and organization, each seeks the common goals of explicitly documenting, in a single framework, the various facets of the system, such as the system's behavior, structure, and history (Craft, 1998). Unfortunately, industry has cited the following broad-level weaknesses with such frameworks.

- Independence from actual risks, which may lead to:
  - Over- or under-securing information assets (or both)
  - Difficulties in measuring the efficiency of security procedures (Chuvakin, 2002)
  - Measurement of security investment effectiveness is largely ignored (Payne, 2001)
  - Answers to the aforementioned questions are difficult to determine (Payne, 2001)

Jamie Carroll (2000) has proposed a potential solution to these weaknesses: metrics. With metrics, a number of advantages are realized (Carroll, 2000):

- Processes become repeatable, more manageable, and may be carried out more frequently on specific systems
- Risk assessments can be performed immediately
- System targeting can be performed more frequently
- Risk assessment processes and results between service providers may become more standardized
- Threat, risk and impact baselines, for similar functional systems, may be created
- Planning, programming and budgeting system inputs, for acquisition and development, may realize improvements

By finding a middle ground between the highly quantitative measures of the late 1970's and the qualitative frameworks currently being used, this research has attempted to broach a topic currently in its infancy (IS metrics) and taken a step toward the fourth generation of IS paradigms (Fletcher, 1995).

FRAMEWORK: METRICS BASED SECURITY ASSESSMENT

The first steps in building the MBSA required a compare and contrast of the SSE-CMM and ISO 17799 standard, resulting in the following tables:

- A matrix defining the areas of overlap
- A matrix defining the strengths and weaknesses of each
- Matrixes illustrating where one model mitigated specific weaknesses of the other
  - The primary SSE-CMM weakness mitigated is that of a lack of defined standards for which to measure against
  - The primary ISO 17799 weakness mitigated is that of a lack of measurement and assessment

Once all tables had been created, the author framed ISO 17799 processes in the SSE-CMM framework, and identified where, within the SSE-CMM process model, the MBSA best fit. The framework is illustrated in Figure 1.

Figure 1. MBSA architecture

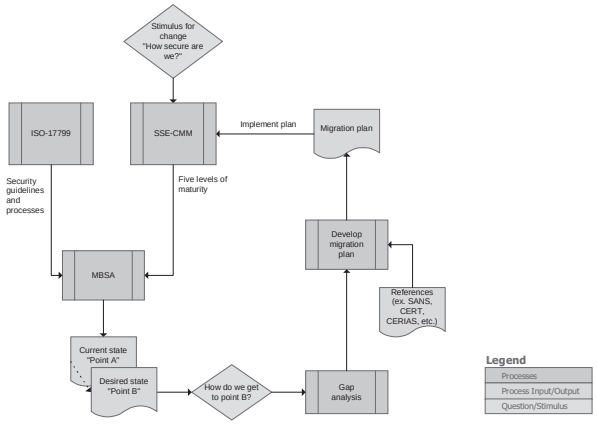

Table 1. Metric sample

Metric	Terms and conditions of employment state employee responsibilities regarding IS and (where appropriate) are continued for a period of time after the employment period
Maturity Level Goal	Level 3
Scale/Rating	0—1—2—3—4—5 N/A Unknown
Frequency	Current Date: Frequency: Next Assessment Date:
Implementation Evidence	Sample Only
Data Source	Sample Only

Constructing the metrics required framing each ISO process in the form of specific, measurable quantities and developing a response scale inline with SSE-CMM parameters. A sample MBSA template and metric is illustrated in Table 1.

Assessing each control is straightforward; for each baseline control, a response indicating the degree to which the control has been implemented is recorded. The two extreme responses are 0 and 5:

- Score a baseline control as 0 if the baseline control is required but has not been implemented in the organizational entity for which responses are being sought and there has been no effort put forth that might ultimately lead to implementation.
- If the control is not required or the question is not applicable to the organization, score it as N/A.
- Score a control as 5 if the baseline control has been fully implemented in the organizational entity for which responses are being sought and the assessor is satisfied with the quality and completeness of that implementation.

Generally, values between 0 and 5 should reflect the extent of implementation. For instance, if the security policy is 20% of the way towards Level 5 maturity, score the control as 1. If the security policy is 60% of the way towards Level 5 maturity, score the control as 3.

Scores can be influenced by varying degrees of implementation within the organizational entity. If one part of the entity has completely implemented a security policy, while another part has rejected that policy and has no plans to develop their own, the control should by scored as a 2 (rounding down to limit the potential for a 'false feeling of security') for the entire organization. Note fractional values are not defined in the MBSA; this promotes a more straightforward alignment with the SSE-CMM.

Assigning scores to controls is most straightforward if they are thought of in the following manner: score 0 being 0% of the way towards full and complete attainment of Level 5 maturity and 5 being 100%. Scores between 0 and 5 signify only partial implementation of the ideal maturity level (Level 5).

Averaging the values of each metric within a given process area (PA), the assessor may report (e.g., to management) their overall assessment and therefore readily identify the level of maturity for each PA within the SSE-CMM. Should the organization elect to assess each process area on an annual basis, the following legend may prove useful; it allows the organization to easily indicate up to four years of maturity within a single assessment document.

- 2002 – Underlined
- 2003 – Highlighted
- 2004 – Box
- 2005 – **Bold**

Within Table 1, the 'Scale/Rating' can be marked according to the previous list, such that past assessments can visually be identified. For instance, in Table 1, the assessor can clearly see the maturity levels attained for the metric; indicating that in 2002 and 2003, the entity was at Level 1. In 2004, the system progressed to Level 2; and in 2005, the goal of Level 3 maturity was attained. Note a similar legend is easily applied to the averages calculated when reporting PA assessments.

Due to time constraints, validation and testing of the MBSA has been delimited from the scope of the research; future scholars should attempt to more thoroughly test and validate this work. To assist in the process, Figure 1 illustrates the MBSA architecture; for which the following six steps have been defined.

1. Enter the SSE-CMM maturity model – the stimulus for change is the question: "how secure are we?"
2. Combine the strengths of the SSE-CMM and ISO 17799 standard – through the areas of identified mitigated weaknesses, the MBSA attempts to account for the SSE-CMM's lack of defined processes and the ISO 17799 standard's lack of measurement and assessment.
3. Determine current and desired state – conducting the MBSA results in a current state definition of IS maturity. Activities such as benchmarking or consultation with local system, environment and technological requirements, should be considered to define a desired state.
4. Conduct gap analysis – a gap analysis should be considered as a means for identifying the processes and requirements to get from the current state to the desired state.
5. Develop migration plan – based on the gap analysis findings, a migration plan should be developed and implemented (per the SSE-CMM process model) according to business need.
6. Re-evaluate IS maturity – after implementing the migration plan, and continuing its progress through the SSE-CMM process model, the organization reaches the step of 'analysis and evaluation,' where it should, again, conduct the MBSA, assess the results (i.e., the 'New current state' after implementing the migration plan) against the 'desired state' maturity level, defined in the initial stages of the framework, and identify potential future actions, resulting in an iterative approach to IS maturity. Note that conducting the full MBSA may not be required; depending on the business drivers at hand, the organization may chose only to assess the changes that were implemented and identify the level of maturity attained by such projects.

Certainly, this is a work in progress that must be cost justified and tested prior to implementation. The research is seen as a point of entry toward the fourth-generation of IS, and may benefit those organizations seeking a measurement tool to finally answer: "How secure are we?"

REFERENCES

Carroll, J.M. *A Metrics-based Approach to Certification and Accreditation*. BTG Inc. July 6, 2000.

Chuvakin, A. (2002, Jan. 28). *Approaches to Choosing the Strength of Your Security Measures*. LinuxSecurity.com. Ret. April 4, 2002, from: http://www.linuxsecurity.com.

Craft, R. et al. (1998, Aug. 6). *An Open Framework for Risk Management*. National Institute of Standards and Technology. Ret. Aug. 27, 2002, from: http://csrc.nist.gov/nissc/1998/proceedings/paperE6.pdf.

Dargan, L. (2002, Aug. 24). Smashing the Milestone. SC Info Security Magazine. Ret. July 2002, from: http://www.scmagazine.com/scmagazine/sconline/2002/article/32/article.html.

Fletcher, S., Jansma, R., Lim, J., Halbgewachs, R. Murphy, M., Wyss, G., *Software System Risk Management and Assurance*, Proc. of the 1995 New Security Paradigms Workshop, Aug. 22-25, 1995, San Diego, CA.

Hopkins, J.P. (1999). *The Relationship Between the SSE-CMM and IT Security Guidance Documentation*. EWA-Canada Ltd., 1-7.

Nielsen, Fran. (2000). *Approaches to Security Metrics*. Ret. August 25, 2002, from: http://csrc.nist.gov/csspab/june13-15/metrics_report.pdf.

Payne, S. (2001, July 11). *A Guide to Security Metrics*. SANS Institute. Ret. March 16, 2002, from: http://rr.sans.org/audit/metrics.php.