Chapter 3.19
Metric Based Security Assessment

James E. Goldman
Purdue University, USA

Vaughn R. Christie
Purdue University, USA

ABSTRACT

This chapter introduces the Metrics Based Security Assessment (MBSA) as a means of measuring an organization's information security maturity. It argues that the historical (i.e., first through third generations) approaches used to assess/ensure system security are not effective and thereby combines the strengths of two industry proven information security models, the ISO 17799 Standard and the Systems Security Engineering Capability Maturity Model (SSE-CMM), to overcome their inherent weaknesses. Furthermore, the authors trust that the use of information security metrics will enable information security practitioners to measure their information security efforts in a more consistent, reliable, and timely manner. Such a solution will allow a more reliable qualitative measurement of the return achieved through given information security investments. Ultimately, the MBSA will allow professionals an additional, more robust self-assessment tool in answering management questions similar to: "How secure are we?"

INTRODUCTION

Information security incidents are on the rise, with new attacks reported daily (for the latest statistics on system related incidents and security breaches refer to http://www.cert.org/stats/cert_stats.html). How have system administrators and security professionals reacted to these new threats? Historically, system owners have rushed to "acquire the latest cure" (Nielsen, 2000). They have tried in earnest to procure today's fix with little thought to the benefit truly gained from such utilities and

or techniques. This approach to system security is changing; that is, the paradigm is shifting toward a model of increased accountability. Security managers are increasingly being held responsible for demonstrating the effectiveness of their security initiatives, for showing that their investments have provided not only value but also greater security to their respective organizations. In short, they are being asked, "How secure are we?" (Payne, 2001).

Answers to this and similar questions are not easy to derive (Payne, 2001). Dating back to the late 1970s and early 1980s when the annual loss expectancy (ALE) calculation was being developed by the Federal Information Processing Standard (FIPS), security professionals have attempted to define security by a single distinct value: ALE (Fletcher, 1995). Since that time, additional information security management tools and documents have been developed. In recent years, a number of guidance documents have been published to assist organizations, both in the public and private sectors, in establishing and maintaining their information technology security programs (Dr. Fletcher has described these guideline documents as third-generation information security tools). Examples of these documents include the NIST Handbook, the CSE Guide, BSI 7799, ISO 17799, and ISO/IEC 13335 (Hopkins, 1999). Unfortunately, problems reside in these guidance tools; specifically, their holistic nature makes it difficult to measure specific information security parameters easily, effectively or efficiently (Payne, 2001).

This chapter proposes a metric-based information security maturity framework constructed from the combination of the ISO 17799 Standard and the Systems Security Engineering Capability Maturity Model (SSE-CMM). While many believe the SSE-CMM to be simply another in the myriad of recently published best practices and general security guidelines (i.e., a supplement to the ISO 17799 Standard as opposed to its complement), their assessment is inaccurate (Hopkins, 1999). The MBSA will illustrate how the SSE-CMM can be used to measure the maturity of the information security practices implemented via the ISO 17799 Standard. The end result will be a self-facilitated metrics-based assessment model that enables organizations, from both the public and private sectors, to accurately assess the maturity of their information security processes. By using the SSE-CMM to measure the maturity of an organization's information security program (specifically the ISO 17799 Standard), the proposed solution will enable professionals to measure in a more consistent, reliable, and timely manner areas for improvement and effectiveness. Furthermore, it will allow a more reliable qualitative measurement of the return achieved through given information security investments. Ultimately, the solution offered in this chapter will allow professionals an additional, more robust self-assessment tool in answering: "How secure are we?"

STATEMENT OF THE PROBLEM

Encouraged by a combination of the terrorist actions of September 2001, the mounting complexity of malicious online attacks, and the increasing realization that unbroken network surveillance, immediate intrusion detection and real-time response strategies are boardroom responsibilities, information security has come to the forefront of corporate and government agendas (Dargan, 2002). However, even with growing media attention and information technology (IT) spending predictions, most of the data seen by Ultima Business Solutions' security consultants suggest that more and more information technology teams are continuously failing in their responsibility to protect their organizations from attack (Dargan, 2002).

Emphasizing the importance of information security, the United States federal government is