A Guide to Security Metrics

Shirley Payne

A Guide to Security Metrics

Shirley C. Payne
June 19, 2006

SANS Security Essentials GSEC Practical Assignment Version 1.2e

Preface

This paper covers the basic aspects of security metrics. If you are interested in learning more about information security metrics and auditing, we recommend taking the SANS SEC410 IT Security Audit & Control Essentials course, available both online and via live classroom training.

The pressure is on. Various surveys indicate that over the past several years computer security has risen in priority for many organizations. Spending on IT security has increased significantly in certain sectors -- four-fold since 2001 within the federal government alone.[1] As with most concerns that achieve high priority status with executives, computer security is increasingly becoming a focal point not only for investment, but also for scrutiny of return on that investment. In the face of regular, high-profile news reports of serious security breaches, security managers are more than ever before being held accountable for demonstrating effectiveness of their security programs.

What means should managers be using to meet this challenge? Some experts believe that key among these should be security metrics.[2] This guide provides a definition of security metrics, explains their value, discusses the difficulties in generating them, and suggests a methodology for building a security metrics program.

Definition of Security Metrics

It helps to understand what metrics are by drawing a distinction between metrics and measurements. 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.[3] Measurements are generated by counting; metrics are generated from analysis.[4] In other words, measurements are objective raw data and metrics are either objective or subjective human interpretations of those data.

Good metrics are those that are SMART, i.e. specific, measurable, attainable, repeatable, and time-dependent, according to George Jelen of the International Systems Security Engineering Association.[5] Truly useful metrics indicate the degree to which security goals, such as data confidentiality, are being met, and they drive actions taken to improve an organization's overall security program. Distinguishing metrics meaningful primarily to those with direct responsibility for security management from those that

speak directly to executive management interests and issues is critical to development of an effective security metrics program.[6]

The Value of Security Metrics

A widely accepted management principle is that an activity cannot be managed if it cannot be measured. Security falls under this rubric. 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:

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

Why Metrics Generation Is Difficult

Many in the security industry will agree that the number of successful security attacks an organization has experienced is not necessarily an indication of how secure that organization is. Luck plays a major role,[7] and how does one measure luck? So, a security manager needs to look beyond the organization's security incident record for indicators of security strength. There are further complications they need to keep in mind, however, in their search for meaningful metrics.

As a case in point, asset value, threat, and vulnerability are critical elements of overall risk and are (or should be) weighed in most decisions having to do with security. Each of these elements poses difficulties when trying to incorporate them into a useful security metric. *Asset value* is the easiest of these three elements to measure; however, certain aspects of value, such as a company's good reputation, are hard, if not impossible, to quantify. Some believe that *threat* cannot be measured at all, since it is the potential for harm,[8] although survey results and other information gathered from external sources could be useful in quantifying threat at a high level. Some progress is being made in objectively measuring *vulnerability*, at least for specific types networked computer devices. For example, the Center for Internet Security[9] has established benchmarks and developed automated tools to detect levels of computer system vulnerabilities. Measurements of other facets of vulnerability, such as degree of understanding of security issues among computer users, remain somewhat subjective.

Security metrics are also hard because the discipline itself is still in the early stages of development.[10] There is not yet a common vocabulary and not many documented best practices to follow. Those pursuing the development of a security metrics program should think of themselves as pioneers and be prepared to adjust strategies as experience dictates.

Building a Security Metrics Program

To facilitate understanding and acceptance at all levels of a new security metrics program, it is advisable to ground the program in process improvement frameworks that are already familiar to the organization. The Dupont Corporation, for example, bases its program on the popular "Six Sigma Breakthrough Strategy", a marketed management process that focuses on defect elimination.[11] The First Union Corporation ties its metrics program to corporate security standards compliance.[12] A representative of Bear, Stearns and Company espouses an audit-based approach that verifies compliance with industry standard control objectives as well as locally defined standards.[13]

Regardless of the underlying framework, the seven key steps below could be used to guide the process of establishing a security metrics program.

1. Define the metrics program goal(s) and objectives
2. Decide which metrics to generate
3. Develop strategies for generating the metrics
4. Establish benchmarks and targets
5. Determine how the metrics will be reported
6. Create an action plan and act on it, and
7. Establish a formal program review/refinement cycle

This seven-step methodology should yield a firm understanding of the purpose of the security metrics program, its specific deliverables, and how, by whom, and when these deliverables will be provided. The steps are briefly described below, and outcome examples, where appropriate, are provided.

Step 1: Define the metrics program goal(s) and objectives

Because developing and maintaining a security metrics program could take considerable effort and divert resources away from other security activities, it is critical that the goal(s) and objectives of the program be well-defined and agreed upon up front. Although there is no hard and fast rule about this, a single goal that clearly states the end toward which all measurement and metrics gathering efforts should be directed is a good approach. A goal statement might be, for example:

Provide metrics that clearly and simply communicate how efficiently and effectively our company is balancing security risks and preventive measures, so that investments in our security program can be appropriately sized and targeted to meet our overall security objectives.

Statements of objective should indicate high-level actions that must be collectively accomplished to meet the goal(s). An action plan should be directly derivable from these statements. A few objectives for the goal above, for example, might be:

a. *To base the security metrics program on process improvement best practices within our company.*
b. *To leverage any relevant measurements currently being collected.*
c. *To communicate metrics in formats custom-tailored to various audiences.*
d. *To involve stakeholders in determining what metrics to produce.*

Step 2: Decide which metrics to generate

Any underlying corporate framework for process improvement, as discussed at the beginning of this section, could dictate what metrics are needed. For example, a "Six Sigma" approach would focus on security processes for which defects could be detected and managed, and Step 2 of building a metrics program would, therefore, be to identify those specific security processes. A compliance-based approach would assess how closely established security standards are being followed. In this case, Step 2 would identify those standards for which compliance should be tracked.

In the absence of any preexisting framework, a top-down or a bottom-up approach for determining which metrics might be desirable could be used. The top-down approach starts with the objectives of the security program, and then works backward to identify specific metrics that would help determine if those objectives are being met, and lastly measurements needed to generate those metrics. For example:

TOP-DOWN APPROACH	
a. Define/list objectives of the overall security program	Example objective: *To reduce the number of virus infections within the company by 30% by 2002*
b. Identify metrics that would indicate progress toward each objective	Example metric: *Current ratio of virus alerts to actual infections as compared to the baseline 2000 figure*
c. Determine measurements needed for each metric	Example measurement: *Number of virus alerts issued to the organization by month* Example measurement: *Number of virus infections reported*

The bottom-up approach entails first defining which security processes, products, services, etc. are in place that can be or already are measured, then considering which meaningful metrics could be derived from those measurements, and finally assessing how well those metrics link to objectives for the overall security program. To illustrate:

BOTTOM-UP APPROACH	
a. Identify measurements that are/could be collected for this process	Example measurement: *Average number of Level 1 vulnerabilities detected per server by department using our xyz scanning tool*
b. Determine metrics that could be generated from the measurements	Example metric: *Change in number of critical vulnerabilities detected on servers by department since last reporting period*
c. Determine the association between the derived metrics and established objectives of the overall security program	Example objective: *To reduce the level of detectable vulnerabilities on servers in every department within the company.*

The top-down approach will more readily identify the metrics that should be in place given the objectives of the overall security program, while the bottom-up approach yields the most easily obtainable metrics. Both approaches assume that overall security program objectives have already been established. If they have not been, defining these high-level objectives is obviously important and a prerequisite.

Step 3: Develop Strategies for Generating the Metrics

Now that what is to be measured is well understood, strategies for collecting needed data and deriving the metrics must be developed. These strategies should specify the source of the data, the frequency of data collection, and who is responsible for raw data accuracy, data compilation into measurements, and generation of the metric.

Although a formal risk assessment is one method for collecting some of the data that might be needed, experts disagree on its value for generating metrics. One line of thought is that quantitative risk assessment provides "close enough" metrics,[14] while another is that risk assessments are not standardized and are too subjective and speculative to provide good comparative metrics over time.[15] There are, however, other suggested sources of data, such as help desk logs, system logs, firewall logs, audit reports, and user surveys.

Early on there were few automated tools available to make data collection, analysis, and reporting cost-effective, but in recent years products have been introduced into the marketplace to make these activities more viable.

Step 4: Establish benchmarks and targets

In this step appropriate benchmarks would be identified and improvement targets set. Benchmarking is the process of comparing one's own performance and practices against peers within the industry or noted "best practice" organizations outside the industry. Not only does this process provide fresh ideas for managing an activity, but also can provide comparative data needed to make metrics more meaningful. Benchmarks also help establish achievable targets for driving improvements in existing practices. A security manager should consult industry-specific data resources for possible benchmarks and best practices, but also may find national and global metrics provided by SecurityStats.com,[16] CIO Magazine,[17] and other services and publications helpful.

Step 5: Determine how the metrics will be reported

Obviously, no security metrics efforts are worthwhile if the results are not effectively communicated. While conventional management wisdom on disseminating information of this nature should prevail, current security metrics literature does reveal some guidance in this area. One analyst, for example, cautions that over-simplification in the name of clarity is a mistake. Executives are accustomed to dealing with financial and other trend lines, so complex security-related data can be valuable to this group if presented well. Graphic representations are particularly effective.[18]

Some metrics may be meaningful only to the security manager and staff and should not be distributed further. Security managers may, however, use other metrics to help trigger needed remedial actions with the organization. For example, a widely distributed metric, such as one that shows levels of vulnerability for each department in the organization, might spawn healthy competition among departments to become the least vulnerable department by the next reporting period -- a security manager's dream!

In any case, the context, format, frequency, distribution method, and responsibility for reporting metrics should be defined up front, so that the end product can be visualized early on by those who will be involved in producing the metrics and those who will be using them for decision-making.

Step 6: Create an action plan and act on it

Now it is time to get the real work done. The action plan should contain all tasks that need to be accomplished to launch the security metrics program, along with expected completion dates and assignments. As mentioned in Step 1, action items should be directly derivable from the objectives. Documenting the linkage of actions in the plan to these objectives is useful, so that no one will lose sight of why a given action is important.

In the same manner that software should be developed, it is critical to include a testing process in the plan. Deficiencies in collected data may, for example, prove some metrics unusable and require reexamination of what is to be measured and how.

Step 7: Establish a formal program review/refinement cycle

Formal, regular reexamination of the entire security metrics program should be built into the overall process. Is there reason to doubt the accuracy of any of the metrics? Are the metrics useful in determining new courses of action for the overall security program? How much effort is it taking to generate the metrics? Is the value derived worth that effort? These and other questions like them will be important to answer during the review process. A fresh scan of security metrics standards and best practices within and outside the industry should also be conducted to help identify new developments and opportunities to fine-tune the program.

Conclusion

The task of developing a security metrics program may seem daunting to some, but it need not be. The seven-step methodology can guide development of very simple metrics programs, as well as highly ambitious ones. In fact, some individuals with experience in security metrics recommend that simple starts be made. They advise managers to do what is easy, cheap, fast, and leverage existing measures and metrics.[19] The important thing to keep in mind is that the metrics generated should be useful enough to drive improvement in the overall security program and to help prove the value of that program to the organization as a whole.

The purpose of this guide is to provide an overview of the current state of security metrics as well as suggestions for developing a metrics program. The following are noteworthy related standards or initiatives that may provide further insight and guidance:

- The International Systems Security Engineering Association's SSE-CMM Project[20]
- The National Institute of Standards and Technology's IT Security Assessment Framework[21]
- The National Institute of Standards and Technology's Security Metrics Guide for Information Technology Systems[22]
- The Department of Defense's Information Assurance Readiness Project[23]
- The ISO standard for Common Criteria[24]

This paper covers the basic aspects of security metrics. If you are interested in learning more about information security metrics and auditing, we recommend taking the SANS SEC410 IT Security Audit & Control Essentials course, available both online and via live classroom training.

[1] Olsen, Florence. "Input: IT Security Spending To Catch Its Breath." Federal Computer Week. 13 July 2005. URL: http:www.fcw.com/article89546-07-13-05 (16 June 2006).

[2] Frank, Diane. "Agencies Seek Security Metrics." Federal Computer Week. 19 June 2000. URL: http://www.fcw.com/article70756 (16 June 2006).

[3] Jelen, George. "SSE-CMM Security Metrics." NIST and CSSPAB Workshop, Washington, D.C., 13-14 June 2000. URL: http://csrc.nist.gov/csspab/june13-15/jelen.pdf (10 July 2001).

[4] Alger, John I., "On Assurance, Measures, and Metrics: Definitions and Approaches," Applied Computer Security Associates Workshop on Information-Security-System Rating and Ranking, Williamsburg, Virginia, 21-23 May 2001: 1-2. URL: http://www.acsac.org/measurement (16 June, 2006).

[5] Jelen

[6] Robinson, Chad. CSO Magazine Analyst Reports. 19, April, 2004. URL: http://www.csoonline.com/analyst/report2412.html (16 July 2006)

[7] Burris, Peter, and Chris King. "A Few Good Security Metrics." METAGroup, Inc. audio, 11 Oct. 2000. URL: http://www.metagroup.com/metaview/mv0314/mv0314.html (10 July 2001).

[8] Nielsen, Fran. "Approaches To Security Metrics." NIST and CSSPAB Workshop, Washington, D.C., 13-14 June 2000: 7. URL: http://csrc.nist.gov/csspab/june13-15/metrics_report.pdf (10 July 2001).

[9] See URL: http://www.cisecurity.org (16 June 2006).

[10] Nielsen: 3.

[11] George, Robert T. "Security Management in the Fibers and Chemicals Industry." NIST and CSSPAB Workshop, Washington, D.C., 14 June 2000. URL: http://csrc.nist.gov/csspab/june13-15/George.pdf (10 July 2001).

[12] Hymes, Pat. "System Security Compliance Monitoring Program." NIST and CSSPAB Workshop, Washington, D.C., 14 June 2000. URL: http://csrc.nist.gov/csspab/june13-15/Hymes.pdf (10 July 2001).

[13] Bayuk, Jennifer L. "Information Security Metrics: An Audited-based Approach." NIST and CSSPAB Workshop, Washington, D.C., 14 June 2000. URL: http://csrc.nist.gov/csspab/june13-15/Bayuk.pdf (10 July 2001).

[14] Nielsen: 7.

[15] Burris and King.

[16] See URL: http://www.securitystats.com (16 June, 2006).

[17] See URL: http://www.cio.com (16 June 2006)..

[18] Berinato, Scott. "A Few Good Metrics," CSO Magazine, 1 July 2005. URL: http://www.csoonline.com/read/070105/metrics.htmlhttp://www.csoonline.com/read/070105/metrics.html (16 July 2006).

[19] Craft, James P. "Metrics and the USAID Model Information Systems Security Program." NIST and CSSPAB Workshop, Washington, D.C., 14 June 2000. URL: http://csrc.nist.gov/csspab/june13-15/Craft.pdf (10 July 2001).

[20] See URL: http://www.issea.org (16 June, 2006).

[21] See URL: http://csrc.nist.gov/organizations/guidance/framework-final.pdf (16 June 2006).

[22] See URL: http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf (16 June 2006).

[23] Bartlett, Terry. "Information Assurance Readiness Assessment." NIST and CSSPAB Workshop, Washington, D.C., 14 June 2000. URL: http://csrc.nist.gov/csspab/june13-15/Bartlett.pdf (10 July 2001).

[24] See URL: http://csrc.ncsl.nist.gov/cc/ (10 July 2001).

Last Updated: May 19th, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Cyber Defence Singapore 2020	**Singapore, SG**	**Aug 17, 2020 - Aug 22, 2020**	**Live Event**
SANS OnDemand	**OnlineUS**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**