Effective Security Metrics

A Guide to Effective Security Metrics

Last reviewed: March 2017

Introduction

In today's economic environment, few, if any, institutions of higher education are escaping the need to prune programs that do not clearly and directly support high priority goals. Investments in information security program are not exempt from such scrutiny, and those responsible for this function may find themselves struggling to demonstrate strategic value and operational effectiveness, an endeavor that has been a significant challenge for the information security profession even in the best of times. What means should be used to meet this challenge? Key among these should be security metrics.

Metrics can provide insights regarding information security program effectiveness, levels of regulatory compliance, and ability of staff and departments to address security issues for which they are responsible. Metrics can also help identify levels of risk in not taking certain mitigation actions and, in that way, provide guidance for prioritizing future resource investments. Because metrics provide concrete facts and a common vocabulary for communicating risks, they may additionally be used to raise the level of security awareness within the organization. Finally, with knowledge gained through metrics, those responsible for information security programs can be better prepared to credibly answer hard questions from their executives and others, such as:

- How do our information security investments help further institutional mission and goals?
- Are we more secure today than we were before?
- How do we compare to others in this regard?
- Are we secure enough?

This guide defines security metrics, describes characteristics of effective metrics, discusses different types of metrics and where they are best used, and provides tips for communicating metrics to executives. Further information and guidance is provided in the "7 Things You Should Know about Information Security Metrics" publication and links to additional helpful references are provided on the EDUCAUSE Security Metrics resource page.

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 of two or more measurements taken over time. 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.

Measurement example: *Number of high severity vulnerabilities detected on Department XYZ's servers by the latest monthly vulnerability scanning process*
Metric example: *Change in number of high severity vulnerabilities detected on Department XYZ's servers in FY2012 as compared to the established FY2010 baseline*

Effective Security Metrics

Effective metrics are often referred to as SMART, i.e. specific, measurable, attainable, repeatable, and time-dependent. To be truly useful, metrics should also indicate the degree to which security goals are being met and drive actions taken to improve an organization's overall security program. In the pursuit of metrics that meet these criteria, it is important to consider:

- how difficult collection of accurate data might be for a given metric;
- the potential that the metric might be misinterpreted;
- the need to periodically review metrics that are being tracked and make changes as needed.

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 an institution'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, although survey results and other information gathered from external sources could be useful in quantifying threat at a high level. Objectively measuring vulnerability, at least for specific types of networked computer devices, is today relatively easy given the number of quality 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.

Risk = Asset Value x Threat x Vulnerability

- *Asset Value* – easiest to measure in some cases, but difficult to quantify certain assets like institutional reputation
- *Threat* – very hard to measure the potential for harm, although information from external sources may be useful
- *Vulnerability* – automated computing device vulnerability tools provide good information, but not all vulnerabilities can be quantified

Regarding potential misinterpretation, consider, for example, the metric often appearing in the popular press that deals with the number of security breaches experienced by a specific entity or industry sector. Many in the security profession would agree that this metric is not necessarily an indication of how secure an organization actually is. Indeed, certain security improvements may reveal security lapses that previously went undetected, and this is a good thing. Although this metric is easy to produce, a security manager should look beyond the institution's security incident record for indicators of security strength and choose metrics that demonstrate true progress toward goals.

Finally, it is important to consider that the effectiveness of a given metric can vary depending upon the maturity of the overall security program and/or specific program component. To illustrate, assume that Institution A has just issued a policy that all mobile computing devices must be encrypted and Institution B has had such a policy in place for three years. During the first twelve months after policy issuance, Institution A would likely find a metric indicating the level of policy compliance to be very helpful. At Institution B, where device encryption is now routine, allocating resources to track the level of policy compliance would likely no longer be important. The next section discusses this tie between program maturity and effective metrics in further depth.

Categories and Examples of Effective Security Metrics

While there are multiple ways to categorize metrics, guidance from the National Institute for Standards and Technology (NIST) does this in a way that is more helpful than simply providing tag names for metric groupings. The Performance Measurement Guide for Information Security (NIST SP 800-55 Revision 1) divides security metrics into three categories and links each to levels of security program maturity. The categories are:

- *Implementation* – metrics used to show progress in implementing policies and procedures and individual security controls
- *Effectiveness/efficiency* – metrics used to monitor results of security control implementation for a single control or across multiple controls
- *Impact* – metrics used to convey the impact of the information security program on the institution's mission, often through quantifying cost avoidance or risk reduction produced by the overall security program

As mentioned earlier, truly useful metrics indicate the degree to which security goals are being met and they drive actions taken to improve an organization's overall security program. Before expending resources producing metrics in any of these three categories, it is essential that goals and objectives of the security program be articulated.

The chart below illustrates the linkages between the metric categories and maturity levels and it provides examples of effective metrics.

Security Program Maturity	***Most Effective Metric Category***	***Examples***
Stage 1: few policies, procedures and controls; little measurement data available	N/A - Should focus first on clear definition of security program goals and objectives	Goals: • Significant reduction in sensitive data stored on desktops/laptops • Require all departments to have mission continuity plans
Stage 2: some policies, procedures, and controls implemented; some measurement data collected	Implementation metrics	• % increase over time of desktops /laptops on which sensitive data scanning tool has been deployed • % increase over time of departments with mission continuity plans
Stage 3: well-established policies, procedures, and controls; measurement data readily available	Efficiency/effectiveness metrics	• # of incidences of unapproved storage of sensitive data found on desktops/laptops over time • % of total departments with updated, tested mission continuity plans
Stage 4: policies, procedures, and controls are well-integrated within the security program and with other institutional programs; measurement data collected as a by-product of business processes	Impact metrics	• Reduction in sensitive data exposures due to stolen or vulnerable desktops/laptops • Outcome of 48-hour power outage in administration building

Metrics for Executives

Executive awareness of security concerns is almost certainly assured when the organization experiences a major data breach. Although such an event often provides a favorable environment for furthering the security agenda, given a choice, most information security professionals would prefer a more proactive approach. Major improvements in an organization's security posture can take a very long time to implement; short bursts of executive attention on security do not provide the sustained support needed for long-term changes. But, just how does one build deeper awareness and appreciation of security issues at the highest management echelon?

While the challenges and approaches for communicating with executives about security extend well beyond the scope of this guide, metrics can certainly play a role. It is important, however, to draw a distinction between metrics that are meaningful to those with direct responsibility for security and metrics that speak directly to executive management interests and concerns. Suggested steps that information security managers can take to identify useful metrics for the executive audience follow.

1. Link security strategies to organizational needs and objectives – Executives may have knowledge of security issues, but not see their linkage to institutional missions and long-range plans. Frankly, the linkages may not be immediately obvious to information security professionals either, but they do exist. Consider, for example, the close connection between protecting electronically stored research data from malicious tampering and an organization's goal to increase research funding. Clearly draw these connections and track metrics related to the security activities that support the linked institutional goals.

Consider that executives' main concerns include issues such as:

- Meeting organizational goals
- Maintaining efficient, uninterrupted operational processes
- Fostering a positive public image
- Complying with legal statutes, regulations, contractual obligations
- Managing risks
- What they need and expect from technology is quite different from what technologists typically focus on.

2. Use metrics not easily misinterpreted – Earlier in this guide the problem that metrics might be misunderstood was covered using the number of security breaches metric as an example. When selecting metrics for the executive audience, think carefully about this potential and how to avoid it. Also, be sure to frame metrics in non-technical terms. Most of us are in the IT profession because we love technology for its own sake, and techno-speak is part of who we are. This can, however, be a serious impediment to effective dialogue with those who do not share a passion for the topic. To avoid squandering hard-won opportunities to connect with executives, metrics should be written in language executives use, not our own.

3. Define and communicate the planned state of security in concrete terms – Ensure that the long-term vision for security, as well as why the vision is important to achieve and how it will be reached, is made clear. Use *implementation* metrics to show progress on new, high visibility and/or high investment security initiatives and use *impact* metrics to show the institutional value associated with previous initiatives already in force.

4. Diligently and transparently report both progress and problems – If efforts to communicate metrics that executives care about are working, these individuals will be much more aware of and engaged in security strategies. They will have "skin in the game" and will want to stay informed and given an opportunity help fix problems should they occur. Send them regular metrics updates and highlight any new related concerns when they emerge.

Examples of effective metrics for executives:

- Percentage of IT budget spent on security as compared to peer institutions
- Change in percentage of mission-critical information assets and functions for which security risk assessments have been completed since institution-wide risk management policy was issued
- Change in ratio of security incidents requiring notification to total security incidents discovered since institution-wide project to minimize collection and storage of Social Security numbers was initiated

Questions or comments? Contact us.

Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0).