CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Initiating a Security Metrics Program: Key Points to Consider

Key Message: A sound security metrics program is grounded in selecting data that is relevant to consumers and collecting it from repeatable processes.

Executive Summary

Those embarking on a security metrics program need to ensure that selected metrics map to organizational objectives. They need to know the difference between good metrics and bad metrics as well as what information they are trying to collect, how they are going to collect it, and how they intend to analyze and report it. Good metrics depend on reliable, repeatable processes and data sources, and use an organizational, enterprise-wide point of view, not solely a system- or IT-centric point of view.

In this podcast, Sam Merrell, a member of CERT's Survivable Enterprise Management team, discusses key points to address when starting up a security metrics program. Sam also provides a comprehensive set of additional resources worth consulting.

PART 1: USING METRICS TO MAKE BETTER MANAGEMENT DECISIONS

Background

Current CERT security metrics work includes providing guidance to U.S. government civilian agencies on how to use metrics to help comply with the Federal Information Security Management Act (FISMA).

FISMA establishes a framework for improving the management of information security controls. One of the most effective ways to implement improved controls is through a comprehensive measurement program, keeping in mind the adage "What gets measured gets done."

Having access to reliable metrics and measurements can result in better management decisions on a range of topics – resource allocation, budget, schedule, and control selection.

Metrics provide insight on whether an organization is meeting its security objectives. Metrics can help determine where best to focus limited resources – in other words, help set priorities for security investments.

What Makes for a Good Metric?

According to Andrew Jaquith's book *Security Metrics: Replacing Fear, Uncertainty, and Doubt*, a good metric is:

- Consistently measured without any subjective criteria
- Easily gathered (collected)
- Expressed as a number or percentage
- Expressed using at least one unit of measure, such as hours or dollars
- Very relevant to stakeholders including those who will be using the metrics information

Bad measurements come from unstable programs and unreliable measurements at each point in time.

Defining a Metrics Program

NIST (U.S. National Institute for Standards and Technology) recommends that a metrics program describe:

- How you're going to collect information
- What information you're going to collect
- How the information is relevant to stakeholders
- How you'll analyze the information
- How you'll report the information

NIST has a series of special publications that describe how to implement and manage a security metrics program. The one that is a final, official publication issued in July 2003 is Special Publication 800-55 titled *Security Metrics Guide for Information Technology Systems*.

Two others in draft form include:

- Special Publication 800-80 *DRAFT Guide for Developing Performance Metrics for Information Security*, issued in May 2006. NIST does not intend to issue this SP in final form.
- A revision to SP 800-55 issued in September 2007

NIST's approach has expanded from an information system-centric approach to a more enterprise-wide, organizational approach, recognizing that the need to protect information extends well beyond any specific computer.

PART 2: CHALLENGES AND FIRST STEPS

Challenges in Building a Security Metrics Program

A good metrics program has to be rooted in stable, repeatable processes – and often these are missing.

A metrics program needs to have well-identified data sources that are reliable and always present during metrics collection. Well-defined policies and procedures can inform these sources – and sometimes these are missing as well.

Organizations often struggle with involving all relevant stakeholders. Sometimes people at one level in the organization attempt to define what needs to be measured for others in the organization. When you then try to feed that information upstream or downstream, you find out that the metrics information isn't very relevant to the end consumers.

Getting Started

Start by looking at the organization's strategic drivers and critical success factors. Map these to daily operations and drive measurement from these operational sources.

Make sure you have repeatable processes from which to collect consistent measures. And make sure these map to the organization's strategic goals.

Understand your security objectives to help determine what you need to measure.

Involve all stakeholders in creating metrics requirements.

Know who your end consumer is.

Evaluate measurement processes used in other part of the organization to see if any of these might be relevant.

Evaluate common measurement approaches such as balanced scorecard, quad charts, and heat maps – but be aware that one size does not fit all so be wary of vendor claims.

Resources

Merrell, Samuel. "FISMA and Metrics." (pdf) Presentation at the Federal Information Assurance Conference. October 25, 2007.

Goethert, Wolfhart & Hayes, Will. "Experiences in Implementing Measurement Programs." CMU/SEI-2001-TN-026, November 2001.

Hinson, Gary. "Seven myths about information security metrics." ISSA Journal and NoticeBored, July 2006.

Jones, Cheryl. "Making Measurement Work." CrossTalk, January 2003.

Elizabeth Nichols-related efforts:

- Clear Point Metrics
- Plexlogic

NIST Special Publications web site

Securitymetrics.org, a community website for security metrics practitioners.

SEI's Software Engineering Measurement and Analysis team publications, particularly relevant for CMMI process improvement efforts.