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

Building a Security Metrics Program

Key Message: Selecting and reporting meaningful security metrics depend on picking topics of great interest, defining the business context, and having access to sound data.

Executive Summary

As a community, we've been talking about security metrics for a long time and continue to be frustrated with ineffective results as we attempt to put a security metrics program in place. The challenges can be daunting given the lack of good data to build upon. That said there are a number of steps business leaders can take to make a strong start with immediate payoff.

In this podcast, Betsy Nichols, Chief Technology Officer at PlexLogic and a faulty member at the Institute for Applied Network Security, discusses why security metrics are tough to select, gather, and collect, and how to get a security metrics program up and running.

PART 1: UNDERSTAND YOUR OBJECTIVES AND THE BUSINESS CONTEXT

Why Security Metrics Are So Tough

Addressing "The What"

You need a clear statement of objectives for measuring and for providing whatever insight or information the metrics are expected to convey.

Clear objectives are often missing or hard to come by. It is not straightforward to determine which metrics are most useful for informing and making decisions.

The industry has yet to converge on a standard set of agreed-to security metrics such as those used in data center service level agreements. These include:

- Mean time between failures (MTBF)
- Mean time to repair (MTTR)
- Availability
- Response time

A useful analogy is the standard metrics used in determining a person's medical condition such as blood pressure, temperature, height, weight, and pulse rate.

In all of these, there is a way to establish a baseline, a goal, how to measure where you are between these, and then interpret the results in a meaningful way.

Addressing "The How"

You need to create tools for automation so metrics are captured in a repeatable way and have clarity and authority. In most cases, these don't exist.

Poorly Defined Objectives

Being able to answer such broad questions as "Are we secure?" or "Are we spending too much?" is not sufficient for determining which metrics to collect. It's like asking "Am I healthy?"

Questions (and objectives) need to be more specific, for example, "Is my blood pressure normal?" It is critical to put the answer in a context that is meaningful for the person asking the question. For business leaders, metrics and the questions they address must be framed in a business context.

PART 2: SELECTING USEFUL METRICS BASED ON RISK

Going Further Than Red, Yellow, Green

We'll likely never get away from a high, medium, low or red, yellow, green type of presentation – business leaders really seem to like these. The message can be understood in a short period of time.

Think of these types of high-level representations as an end product derived from supporting quantitative data.

As an example, take a look at the TJX security breach (unauthorized disclosure of credit card and Social Security information for more than 90 million individuals over a wireless network).

If your board of directors asks "What is the situation here? Could this happen to us?" a red, yellow, green picture of where you stand with respect to wireless security could be an effective form of communication.

In building the supporting data, keep in mind that security is all about risk management and that red, yellow, and green are an expression of the organization's risk tolerance.

A structured risk analysis defines areas of unacceptably high risk as a four-tuple:

- The vulnerability
- A threat against that vulnerability
- The impact if the threat is successful in exploiting the vulnerability
- The value of the asset at risk

All of these can be measured. The results of the risk analysis can inspire what metrics you want to focus on first.

Selecting Useful Metrics

The first requirement for a good metric is that it be topical (currently of interest and related to a particular topic).

The second requirement is that there is data to back it up. Try to use existing data and keep in mind that metrics really are all about data.

Some specific metrics that are useful include:

- Security budget as a percentage of overall IT budget
  - Advantages: Easy to understand, generally of high interest to executives
  - Disadvantages: The definition of security budget is typically fuzzy
- Where the CISO fits in the organization (hops to the CEO; number of board appearances per year)
  - Advantage: Can convey the importance the organization places on information security; a proxy for influence
  - Disadvantage: Doesn't really eliminate cheap talk – placing a CISO at a high level as a figurehead

Defining and collecting metrics based on administrative groups (such as divisions or business units) can be useful in allowing leaders to compare across groups, and can stimulate a little healthy competition in the process.

PART 3: CHALLENGES AND GETTING STARTED

Challenges

- Leveraging risk analysis: Often a risk assessment has not yet been done. Getting the structure in place to perform one and take action on the results can be a challenge.
- Being able to identify authoritative sources of data that can be readily accessed: Getting people to share data can be challenging. There can be disagreements about what data is authoritative for a particular subject and about data sources.
- Putting a program in place that is formal: with accountability, assigned people, and having tools that gather and produce good data in a repeatable way.

Getting Started

Seek a topic of great interest as a starting point such as a retail organization's wireless configuration. This can help in keeping business leader attention and often produces useful short term results.

Make sure the selected metrics can be repeatably gathered and reported over time to reveal trends. Absolute numbers are hard to come by.

Consider taking advantage of the connection between metrics and process management. The SEI's CMMI (Capability Maturity Model Integration) is one example of a process model (for software development).

The process perspective can be useful in exploring, for example, the connection between security flaws in software and security incidents in applications.

More mature processes typically have better instrumentation that can be used for collecting useful metrics.

A focus on process tends to break down silos and can bring about integration across multiple sources – correlating what's happening in one part of the organization with another.

Automation that supports metrics gathering and reporting must be really good at data integration.

Resources

Swanson, Marianne, et al. Security Metrics Guide for Information Technology Systems (NIST Special Publication 800-55). Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, July 2003.

Center for Internet Security

Computer Security Institute

SANS

BITS Financial Services Roundtable

Common Vulnerabilities and Exposures

NVD (National Vulnerability Database) Common Vulnerability Scoring System

Jacquith, Andrew. Security Metrics: Replacing Fear, Uncertainty, and Doubt. Addison-Wesley, 2007. Betsy Nichols was the primary author of Chapter 7 Automating Metrics Calculations.

Berinato, Scott. "A Few Good Metrics." CSOonline.com. This article provides recommendations from Andrew

Jacquith.

Securitymetrics.org