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

Getting to a Useful Set of Security Metrics

Key Message: Well-defined metrics are essential to determine which security practices are worth the investment.

Executive Summary

We all react to numbers, from sporting event scores to our personal health scores. Metrics are essential for making well-informed decisions and directing energy and attention, particularly since resources are almost always limited. As a security community, we truly do not know which practices help reduce the number and severity of security breaches. Several efforts are making progress toward this objective.

In this podcast, Clint Kreitner, president and CEO of the Center for Internet Security, discusses the challenges and opportunities in creating a common set of widely accepted security metrics that business leaders and security professionals can use to make better informed decisions.

PART 1: METRICS AS A MEANS FOR DIRECTING ATTENTION AND ENERGY

Metrics as a Business Enabler

Metrics are helpful in determining where to direct the efforts and energies of an organization, and in focusing staff attention on what's important.

Metrics cause staff to ask questions about how their efforts contribute to, for example, financial performance and meeting business objectives.

Visible metrics reporting fosters understanding, engages staff, and promotes learning.

Metrics help focus attention and energy, and help leaders decide where to take action.

Information Overload

With respect to information security in particular, there are an infinite number of things to examine, and we're all suffering from too much information.

Winnowing down to a set of key metrics helps make sense of all of this. We understand and use financial statements to make financial decisions; we need the equivalent for information security.

Growing Interest in Security Metrics

Business leaders are demanding that security professionals justify the money they are spending.

Security professionals are unable to make a convincing case to their managers. The majority have very little idea of what security practices are most cost effective in terms of money spent vs. protection provided.

The growth in U.S. federal and state personal information disclosure laws is providing additional pressure on business leaders to pay attention and take action. They need to have a reasonable explanation of what they are doing in the event of a legal suit.

Metrics provide significant value in addressing these issues. Leaders need to apply the same rigor to security as they do for employee safety in a manufacturing setting.

PART 2: SOME CHALLENGES, AND WORK IN PROGRESS

Tough to Make Real Progress

The magnitude of the information protection challenge is unprecedented in human experience.

We are all interconnected and information can flow from one point to another anywhere on the planet in the blink of an eye.

Huge amounts of valuable information are stored on small physical devices that are easily lost or stolen.

Business executives and system administrators are a world apart in terms of their conceptual frameworks and language.

Security professionals, for the most part, do not know how to frame their arguments in terms that are meaningful for business leaders, for example, information security as a business enabler or disabler of product quality, customer satisfaction, customer trust, and profit.

Promising Efforts

Starting in 2003 under the direction of U.S. Congressman Adam Putnam, the Corporate Information Security Working Group developed a set of 99 metrics that enterprises could use. These are divided into governance metrics (12), management metrics (42), and technical metrics (45).

The U.S. National Institute of Standards and Technology (NIST) has published a series of special publications on security metrics (including SP 800-80 *Guide for Developing Performance Metrics for Information Security*, SP 800-55 *Performance Measurement Guide for Information Security*, and SP 800-53 *Recommended Security Controls for Federal Information Systems*).

Securitymetrics.org, under the leadership of Andrew Jaquith, represents the thinking of leading researchers in the field.

The Center for Internet Security Consensus Metrics Initiative

CIS is leading a community project of thought leaders in security metrics to:

- define and reach consensus on a small number of meaningful security metrics
- build and provide a database infrastructure where users can submit their values, and then use the results to compare their data with generated distribution curves

The intent is to eventually be able to correlate the use of certain security practices with a reduction in the frequency and impact of security breaches (as one example).

Participation in this project is free. Contact Clint at ckreitner@cisecurity.org if you would like to participate.

PART 3: WHERE TO START

Today's Current State

As a community, we honestly do not know what security practices are helping solve the problem and which ones are most cost effective.

Moreover, we keep generating more lists of practices and controls with little guidance on how to select those that are most meaningful based on business objectives.

Some Useful Metrics

These include:

- the percent of breaches that were discovered by internal controls: Breaches are often revealed by outsiders, intruders with a wide range of motives, customers, and business partners, to name a few. Raising the percentage of breaches discovered by internal controls tells us that controls are working.
- frequency and damage caused by security breaches
- time to recover from a security breach
- metrics on the extent of use of specific security practices such as patching, standard software images, and policies for standard configurations.

Correlating each of these metrics to the presence, absence, and degree of security breaches and breach impact helps leaders better understand if their security investments are paying off.

Information Technology Process Institute

ITPI has done extensive research in identifying the characteristics of high, medium, and low performers in terms of

- mean times between incidents (high performers have long mean times)
- mean times to fix (high performers have short mean times)
- amount of unplanned firefighting work (high performers have low levels)
- ratio of systems to system administrators (high performers have high ratios)

ITPI's work reveals that disciplined change and configuration management are predictors of a stable and security computing environment.

Gene Kim's podcasts that describe this work are Change Management: The Security 'X' Factor" and "Connecting the Dots between IT Operations and Security."

Resources

Jaquith, Andrew. *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Addison-Wesley, 2007.

Corporate Information Security Working Group. "Report of the Best Practices and Metrics Team." Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Government Reform Committee U.S. House of Representatives, January 10, 2005.