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

Using Benchmarking to Make Better Security Decisions

Key Message: Benchmark results can be used to compare with peers, drive performance, and help determine how much security is enough.

Executive Summary

In the absence of defensible, concrete, quantitative data, performance benchmarks can be used to better determine how an organization is doing in comparison to peers and as compared with an accepted best practice or standard [Nichols 07]. Benchmark results can provide hard evidence of competitive advantage or help identify areas for improvement if performance falls short.

In this podcast, Betsy Nichols, Chief Technology Officer at PlexLogic and a faulty member at the Institute for Applied Network Security, discusses the benefits and challenges of benchmarking and how benchmark results can contribute to making better-informed security investment decisions.

PART 1: WHAT IS BENCHMARKING AND WHY IS IT USEFUL?

Defining Benchmarking

This podcast compliments Betsy's first podcast on Building a Security Metrics Program.

The purpose of benchmarking is to define a point of reference for measurement. It is all about making comparisons.

There are several types of comparisons for benchmarking purposes:

- Best practice: define “perfection” and determine how far your practice deviates from it.
- Normative: measure a group of people and determine what is typical for the group, whether you are above or below the mean, or whether you are in a certain percentile.
- Timing: use benchmark results in real time to detect anomalies from a norm and take corrective action; use benchmark results over time to aid in making better decisions.

Having a benchmark as a reference point allows an organization to put its metrics in a meaningful context.

Using Benchmark Results

Benchmark results can be used to:

- provide hard evidence of a competitive advantage, to compare your performance with peers (for example security budget per employee can be used to demonstrate an organization's level of commitment to security)
- identify areas that require improvement, where perhaps you don't compare so well to your peers
- defend proposed budget or staff expenditures
- drive performance improvement and measure it
- communicate performance to executives in a crisp, concise manner.

Overall, benchmarks provide information that will lead to better decisions and, in turn, to a better IT security program.

Benchmarks can assist in more meaningful, business-based practice selection and in making risk-based decisions, given that you can't secure everything.

PART 2: BENCHMARKING CHALLENGES AND SOME "WORKS IN PROGRESS"

Major Roadblocks and Challenges to Security Benchmarking

The first challenge is arriving at crisp, unambiguous definitions of what the benchmark will be, including defining how to compute the benchmark, what precise data is required, and what does or does not count.

The second barrier is having a trusted third party that can reliably collect, compute, publish, and protect the benchmark's integrity, confidentiality, and accuracy. The benchmark needs to sustain itself as a business for the third party.

The third barrier is market gravitas - market pull or some meaningful market driver or business basis for the benchmark results. For example:

- The Nielsen rating system for television programming provides ratings that allow a media outlet to charge higher advertising fees.
- The College Board conducts SAT examinations, the results of which can serve as a predictor of success for in-coming college students.
- Moody's rating system for financial institutions uses higher ratings to predict financial success.

Market gravitas is likely the most challenging roadblock to overcome of the three.

Data Sharing and Protecting Sensitive Benchmark Data

Can I conduct meaningful benchmarks without fear of losing privacy or data confidentiality? The answer is yes – and no.

- Yes: It is possible to protect the privacy of individual companies, business units, or people.
- No: Public benchmark results do not necessarily protect the characteristics of the group as a whole.

Example:

When measuring account latency (the mean, elapsed time (hours) between an employee's termination from a company and the removal of all employee IT access to accounts):

- Yes: The benchmark process could protect the transfer and storage of results from participating companies, as well as company statistics and comparison with peers. Companies that performed well may even choose to reveal their results.
- No: By example, if a company reported that it was in the top 5% for account latency but its latency was 3 days, this information about the peer group as a whole could be used by attackers as a window of opportunity.

That said, a forward-looking peer group may say "Let's allow this information to come out. It's going to drive improvement."

Building Trust Relationships: Some Examples

Federal Information Sharing and Analysis Centers (ISACs) are making good progress in building trust relationships in specific market sectors such as the FS-ISAC (financial services) and the MS-ISAC (multi-state).

Currently ISACs are not benchmarking per se, but do share cyber and physical threat data.

The federal mandate for ISAC formation and the relationship with the U.S. Department of Homeland Security facilitate these trust relationships.

The Computer Security Institute conducts an annual survey which presents a comparison of peers.

The Center for Internet Security provides best practice benchmarks for a wide range of operating systems and applications. Their benchmark results have been sustained over a long period of time with a track record of continuous improvement

---

PART 3: KEEPING BENCHMARK DATA UP TO DATE AND GETTING STARTED

Keeping Benchmarks Current

This can be challenging. If the benchmark data is based on technical details that change frequently, then metrics that are collected need to be expanded to reflect new technologies.

As technologies become more widely deployed, thus eliminating some risks, benchmarks need to be adjusted to reflect this. Virus management and firewalls are two examples.

If there is a natural market incentive (and business case) for keeping benchmark data up to date, this is ideal.

Getting Started

The best place to start is with an internal benchmarking program that is an adjunct to a metrics program. This can be used to compare, for example, one business unit's performance with another or one technology with another.

An internal benchmarking activity is advantageous as you can get started without having to coordinate with peer organizations. A company can identify useful benchmarks, perform them, and use the data to start an activity with market peers.

Benchmarks can be effectively used internal and externally to stimulate healthy competition.

Resources

Building a Security Metrics Program by Betsy Nichols, February 2008.

More on the Center for Internet Security's benchmarking efforts: Reducing Security Costs with Standard Configurations by Clint Kreitner, August 2007.