SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

Finding Value in Security Benchmarking: A Current State of Comparison Research in the Security Industry

By George Campbell and Kathleen Kotwica, Contributing Editor

Executive Summary

What is Benchmarking?

Benchmarking compares practices or processes against others to evaluate quality and resource allocations such as personnel or costs. It is also used to ascertain practices or processes that others are doing well and that may fill a known gap in the sponsoring organization. In the particular case of best practice benchmarking, managers identify the best firms in their industry, or in another industry where similar processes exist, and compare the results and processes of those studied to one's own results and processes. In this way, they may gain insight into the particular processes that explain why these firms are successful.

Much of the "benchmarking" that we frequently see in the security management space tends to be one-to-one comparative surveying on data-points rather than the more rigorously analytical practice of business process performance examination.

Gathering Benchmarking Data

Our experience reveals that very useful and actionable data can be gleaned from comparative surveys when the objectives are clearly focused. Because benchmarking can be applied to any business process or function, a range of research techniques may be required.

Benchmarking data can be obtained from the following resources:

- Internal Departments
- Public Sector
- Industry Sources
- Practitioner Experience

Current State of Security Benchmarking

A variety of factors confound the comparison of security-related data, even among peers,[1] that would seem to have directly comparable security missions. For example, unless well understood, security benchmarks do not provide accurate cost comparisons and actionable conclusions. Companies aggregate costs differently, apply widely disparate methods of assigning security costs across revenue and cost centers, and have significant costs in purchased service accounts that can complicate one-to-one comparisons.

Also, security programs vary widely because of organizational structure, scale, assets, regulatory needs, risk awareness, and risk tolerance. Companies with regulatory requirements, such as those in the defense sector, have significant security program costs and operational drivers that are totally foreign to high tech or manufacturing firms, which might otherwise be

[1] The Business Performance Improvement Resource (UK) found 50 percent of companies engaging in benchmarking had significant difficulties in comparing data.

seen as functional "peers." Finding common links among participants can facilitate comparability.

The immediacy of a threat provides another spin on an organization's risk appetite. A company that has specific, more recent, and more severe experience with security threats will likely devote more resources to protection activities.[2] And an increasing number of companies have found that security can be a market differentiator and deserves a specific suite of services and related costs that "peers" may not desire. Cultural and shareholder service expectations can also be a factor. For example, security services in a privately held company may be more apt to reflect and respond to the owners biased concept of "protection" than that of a publicly traded company.

Assessing Benchmarking Data

What action should be taken if a benchmark partner in the same industry has two times the security cost as a percent of revenue versus the sponsoring company? Is its security function that much more cost-efficient or simply experiencing less risk, thus, less pressure for security spending? Or is the company's appetite for risk significantly greater? These are valid (and accepted) measures but, standing alone, are not *actionable*—the primary value of the benchmarking process. As a result, consideration needs to be given to key performance indicators (KPIs) and key risk indicators (KRIs). Others include Key Risk Indicators (KRIs) and Security's Balanced Scorecard.

Managing Benchmarking Results

Many limitations have to be addressed if benchmarking is to deliver results that can be effectively used to direct measurable security process improvements. Several limitations follow, accompanied by approaches that can be used to manage them:

- Definitional limitations
- Limitation on data specificity
- Size limitations.
- Confidentiality limitations
- Sector limitations
- Organizational variability limitations
- Limitations in process cost, time, and effort

Actionable Benchmarking

Simply gathering a variety of business and organizational data in a collaborative, collegial setting is a perfectly appropriate method for comparative analysis. But it leaves significant voids in relevance and actionability, many of which have been noted

[2] As we saw a few years after 9/11, this trend has definable shelf life.

throughout this review. Actionable benchmarking data demand a legitimate context: what is the take away from a result that shows a markedly lower cost per “whatever” or the possibility that a peer is twice as efficient in some measure?

Security executives seriously interested in learning best-in-class business and security practices should plan on deeper dives into a well-planned survey that has been pre-sold with targeted participants. The notion of “collaboration” should be an incentive for partners to learn as well.

For the full version of this report, please contact us at contact@secleader.com

About the Security Executive Council

The Security Executive Council (SEC) is the leading research and advisory firm focused on security risk mitigation. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year "retained" services agreements (Tier 1 Security Leaders™). Tier 1 Security Leaders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us for a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us: contact@secleader.com
Learn more: www.securityexecutivecouncil.com