# Benchmarks Aren't Magic, They're Tools

By Bob Hayes

By Kathleen Kotwica

Security executives frequently come to us to request assistance in benchmarking their processes or performance metrics with similar companies. Usually we find that their interest is at least partially driven by a strong push from management. Business leaders recognize benchmarking as a proven business practice that can identify competitive strengths and vulnerabilities as well as opportunities for improvement. Benchmarking can inform corporate goal-setting and can play a significant role in strategic planning.

But while the demand for performance measures has trickled down to the security function, the appreciation for them hasn't always come along for the ride. Too many security leaders create or find benchmarks for the sole purpose of appeasing their bosses rather than from an earnest desire to use these tools to explore what others are doing, address potential gaps and add value. When management asks for specific benchmarks, they simply gather and present the information requested rather than thinking about, or asking, why and how that information is important to the business of security.

This causes two problems. One: Unless security leaders analyze the benchmark data they've collected, they will be unable to glean much significant insight from it. Comparing numbers alone isn't enough. Unless security leaders look beyond the numbers to consider all the potential explanations of why their program varies from the average, they'll still be missing critical insights.

For example, say you've developed or acquired a benchmark report on ethics hotlines. After reading its assessment of reporting rates, you determine that your organization, given its size and industry, should be receiving eight to nine calls per 1,000 employees. You're only receiving three per every 1,000. This result may seem to clearly indicate that your organization has far fewer compliance issues than its peers and competitors. While that may be so, it's not the only possible explanation. You'd likely receive fewer calls than average if company employees were being intimidated by their managers into keeping mum about misconduct concerns. Or perhaps your awareness program isn't what it should be.

Benchmarking without proper analysis is also likely to lead to some discomfort when management asks what the benchmark says about the performance of security in their company. Is it good, bad, average in comparison with others? Without prior examination and serious thought, this question can't be honestly or adequately answered.

The second problem: The benchmarks management is requesting may not be the right ones. When asked for benchmarks, too few security leaders respond by asking why they want this data. What is the driving force behind the request? Often management sees there's a problem somewhere and they want to get to the bottom of it, but they don't necessarily know the right questions to ask to get there. Knowing the motivation for their benchmarking request could open a gateway for the security leader to collaborate with management to develop a set of benchmark questions that are more likely to uncover helpful information. (What's more, asking about the driver for benchmark requests could shed light on other problems – poor communication with management, a misalignment between security goals and corporate goals, or lack of confidence. Recognizing these problems is the first step to dealing with them.)

Benchmarks only provide their full benefit when they are planned carefully by balancing what the business is looking to discern with what is important to you, the security leader and your department. Absent this, they may get you some short-term recognition, but it won't be long before management comes back asking for more and more benchmarks. You need to get at the real root of the request.

In response to the numerous requests for benchmarks, the Security Leadership Research Institute has just released its first major report, the *Corporate Security Organizational Structure, Cost of Services and Staffing Benchmark*, an attempt to gather the types of data that are typically needed or asked for. You can benefit from this endeavor by joining the SLRI (no fee is required) for the next round of data collection. In the meantime, you can download an executive summary of the report here: https://www.securityexecutivecouncil.com/spotlight/?sid=26697.

If you decide to practice better benchmarking, your business and your function won't be the only beneficiaries. We've seen one carefully developed benchmarking study result in the requesting security executive receiving a major promotion to put him in line with the security leaders at like organizations. A similar study prevented a security leader's role from being downgraded because it showed that other companies in the sector rated security as a highly valued function. SECURITY

**About the Authors:**
Bob Hayes is Managing Director of the Security Executive Council. He has more than 25 years of experience in security, including eight years as the CSO at Georgia Pacific and nine years as security operations manager at 3M. Kathleen Kotwica, PhD, is EVP and Chief Knowledge Strategist for the Security Executive Council. She develops strategies and processes to identify, store, understand, build upon, and disseminate the Council's Collective Knowledge™ and insights. To learn about becoming involved, e-mail contact@secleader.com or visit https://www.securityexecutivecouncil.com/sm.