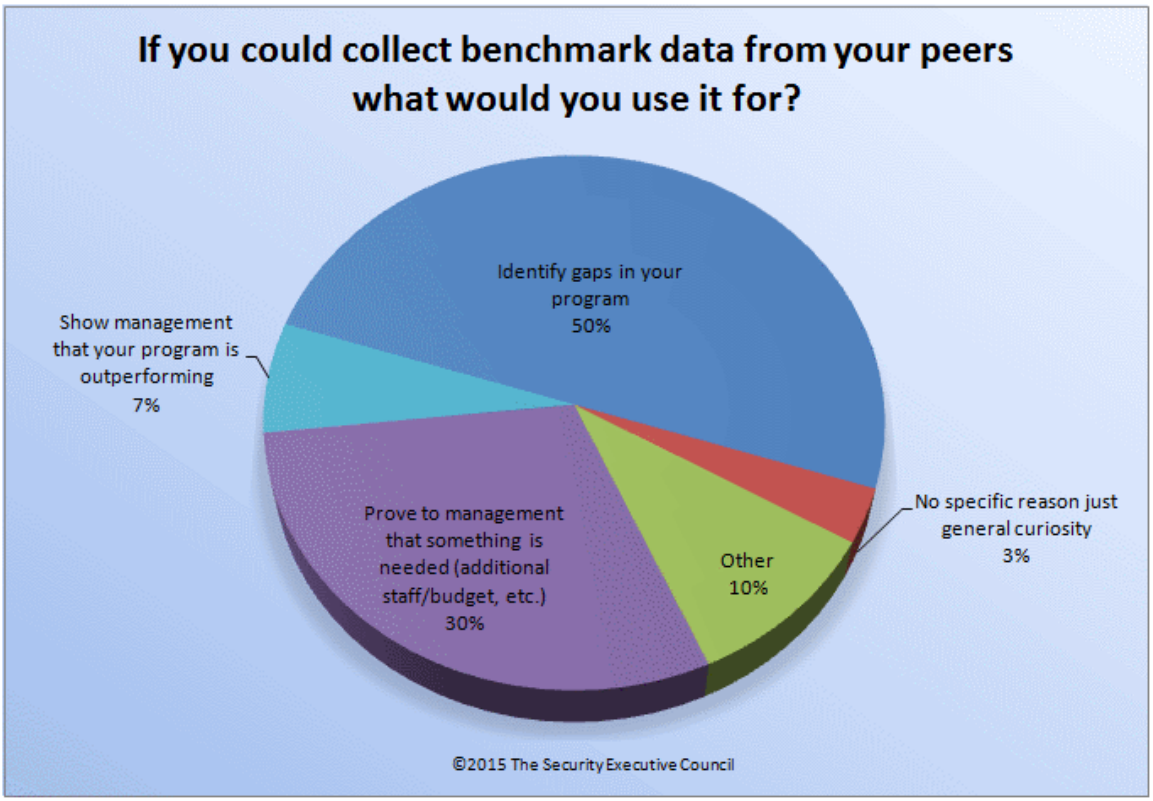
SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Demonstrating Value > Measuring Value >

What Benchmark Data Do You Want?

Created by the Security Executive Council

Almost all security and risk professionals will want to see benchmarking results if given the opportunity. However, the reasons they give for viewing the results can be widely diverse. In this Security Barometer we wanted to take a closer look at those reasons for gathering benchmark data. More specifically we asked security practitioners what benchmarks they would like to gather from their peers and what it would be used for. The results can be seen below:



If you could only pick a handful of the most impactful data, what data would you want to gather from your peers to compare your program?

The second part of this Security Barometer gathered some information about what security practitioners wanted to benchmark against. We thought you might be interested in seeing a list of selected responses to that question to spark some ideas for your metrics program:

- FTE's vs Crime Rate, Incidents per capita, Incidents in facility vs outside facility, Calls for service
- Physical security OPEX to revenue, FTE headcount to revenue, OPEX to employees
- Shrinkage
- Security program coverage compared to company security risks
- Volume of $ in counterfeit seizure versus company sales
- Cable and goods in-transit theft
- Number of resources to perform the job in relationship to tasks required
- Metrics, budgeting, Risk information
- Incident type trends, internal compliance by employees, cost / benefit analysis for overall Security program.
- Security incidents per adjusted patient day, Annual security cost per 1000 patient days, Security service calls per daily guard hour, Workplace violence incidents per 100 employees
- Violent events, Staffing levels, Call volume
- Cost of providing security service, Cost by program, Cost by staff member, Number of reportable incidents
- Total Time spent on service calls by task, Emergency and or routine response times.
- Calls for service data, Citizen satisfaction, Sustained complaints, Response times to critical alarms, Officer retention statistics.
- Budget limitations per site/facility
- What the security staffing is in relation to the number of personnel they are responsible for; the physical size of the properties; urban versus rural; and the number of buildings.
- Security budget
- Is there a formal security awareness program and if so, the participation+pass rates - Number of detected PUA/Malware/Virus on endpoints over a given period of time - Assuming scale of 1-5 with 5 being most critical, % breakdown of category 3-5 vulnerabilities from the vulnerability management program and avg time to remediate them
- 1) headcount per issue covered; 2) budget breakdown, including for training; 3) if their roles have been elevated to direct report to CEO;
- Losses, robbery,
- Demographics (size, scope, services, locations) Cost of security (% revenue, FTEs) Services provided (time per activity, %) Incidents

Reference Materials on Benchmarking that You Can Use

Here are a few articles that may help you on your quest for benchmarking for your program:

Garbage In" Can Cost You Your Job
Security practitioners and executives today have few options for collecting or accessing accurate, usable information. Currently there are four categories of information out there for security practitioners to draw from. In order of validity and rigor, they are: personal opinion, ad hoc benchmarking, selective and vetted benchmarking, and research.

Benchmarks Aren't Magic, They're Tools
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.

Enterprise Security Metrics: A Snapshot Assessment of Practices
This report provides a snapshot of the use of metrics in corporate security management. It includes information on the current state-of-the-art of various models of benchmarking and security metrics, types of metrics, judging the maturity of security metrics programs as well as challenges and opportunities for those undertaking security metrics programs. This report specifically summarizes our learned experience from corporate security measures and metrics initiatives.

Visit the Security Executive Council website for other resources in the Demonstrating Value: Measuring Value series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com

Website: https://www.securityexecutivecouncil.com/

