Marking The Yardstick

BENCHMARKING CAN HELP TO ANALYZE SECURITY EFFORTS, BUT THE DATA HAS TO BE COLLECTED FIRST

BY KATHLEEN KOTWICA AND MARLEAH BLADES

Let's say you're asked to prove the effectiveness of one of your security programs or initiatives to senior management. Or perhaps you need to develop an appropriate program budget, or improve protection in a certain area. Maybe you're simply evaluating your security program to find out what you're missing.

How do you do any of these things?

If you conduct regular risk and vulnerability analyses and you have a security measures and metrics program in place, you have made some important steps. But what if someone—your CEO, for example—were to ask you, "Is your security program one of the best?" As a diligent security professional, you probably have asked yourself that question before. The data you get from your metrics program and analyses is invaluable, but "good," "better" and "best" are comparative terms; you can't use them unless you are judging two or more things side by side.

If you could prove your program is good, better or best, you might have an easier time securing support and funding for security initiatives, and you could easily demonstrate due diligence in case of a breach or lawsuit. If you could prove your program is bad, worse or worst, you would be able to see exactly where you need improvement, and you would again have an easier time demonstrating to senior management the need for funding and support.

In industries such as IT, a director or executive can measure his or her program against the yardstick of a standard or IT industry guideline and say, "Yes, we meet the requirements listed here, so we can say our program is good." But for corporate security, there are no such industry standards. There are plenty of regulations and guidelines that impact various components of corporate security, such as the handling of sensitive financial documents, screening of cargo and placement of life safety equipment, to name a very few. But there is no yardstick labeled "corporate security" that lays out what every security program in every company in every industry should look like.

Right now, the only way a security director can prove the comparative quality of his or her program is to stand it next to the security programs of other companies and judge its performance and completeness against theirs. This is basically what security benchmarking is. And it isn't easy.

Circle of friends

Benchmarking among a few peer companies—working with other security directors you know to discuss programs and risks—may help you see how others are dealing with emerging threats, or why other programs have gained support for types of initiatives that have foundered in your company. Benchmarking at this level cannot often provide a great deal of data, and since it involves only a few companies it doesn't amount to the discovery of best practices. Even within single industry segments, security functions and corporate goals are often unique compared from company to company, and it may be hard to find peers whose programs would provide an appropriate comparison. This type of informal benchmarking also requires confidence that your peers would not disclose any details you provide them. However, even benchmarking at a low level can uncover gaps in your program that can greatly enhance your company's security, so it's well worth the effort.

Need for industry-wide effort

If the security industry were able to create and collectively support a wide-ranging, broad benchmarking effort that reached large numbers of security practitioners and aggregated the data they provided, it would be able to provide much more information than small-scale, peer-to-peer comparisons.

Many organizations have attempted to facilitate security benchmarking at a higher level, asking a large number of security practitioners to respond to short, single-topic surveys that give a glimpse into how the industry as a whole deals with a particular issue. While these projects can be useful in a narrow sense, they provide limited information.

Many practitioners are concerned that their information will be used for marketing purposes if they respond to surveys from some sources, so the respondent pool isn't as big or as well-rounded as it could be. Also, since these surveys often focus on a single topic or even subtopic — workplace violence or insider theft, for instance — they only provide insight into that single element of the security program or threat.

The fact that numerous organizations are regularly sending such surveys poses problems as well. For one thing, the data is not collected in a single place for future reference because it is not shared among surveying organizations, so the benefit of the benchmarking never reaches beyond a single survey. In this sense, every organization that attempts benchmarking is re-inventing the wheel with each survey. Secondly, security practitioners are bombarded with surveys, often on duplicate or similar topics, and many of the surveys simply go straight to the trash bin.

Single resource in the works

A single database that aggregates anonymous information from a significant number of vetted security practitioners is needed in order to properly assess what's really going on in the security function. The Security Executive Council's International Security Research Database was created to serve that function. Its purpose is to collect data on the elements that make up security—including physical security, health and safety, disaster recovery, information protection, fraud, embezzlement, globalization and regulation issues—and to allow the industry to connect that data together.

The database is not limited to a single topic but looks at the whole world of enterprise risk management. So far, the Security Executive Council (SEC) has used the database to study the following issues:

- Security's connection to the enterprise risk categories that are of highest concern to the corporate board
- Regulations and compliance, including corporate ethics
- A baseline for an effective awareness program
- Security program performance metrics
- A baseline for an effective international security program
- Security titles and reporting

This is only the beginning of a long list of topics the database will include. As the initiative grows and more data is added, the International Security Research Database should become a live system that will be able to provide security professionals with data for their own benchmarks upon request. To assist in this endeavor, the Security Executive Council is also launching a new research arm dedicated to providing security program documentation and research.

The most recent International Security Research Database benchmarking survey dealt with the collection of performance metrics, and results were released in late June. At this time, only SEC members and vetted benchmarking survey participants receive the full results report. Some highlights:

- A majority of respondents conduct incident after-action reviews/lessons learned (85 percent).
- More than half of respondents noted that the background investigation process in their company is managed by Human Resources and the data is not available to security (54 percent).
- Respondents in Fortune 500 companies were more likely to track corporate security incidents than respondents in the Fortune 50,000.

Such data, when rolled into a comprehensive database, will help security practitioners justify programs to management and provide the best security available to their companies, but only if more practitioners become involved in this benchmarking initiative.

To be included in the next International Security Research Database survey, which authorizes you to receive full survey results, contact **contact@secleader.com**. ■

KATHLEEN KOTWICA is vice president, research development of the Security Executive Council, a cross-industry professional organization of security executives devoted to advancing strategic security practices. MARLEAH BLADES is senior editor for the Council.

The Security Executive Council regularly shares the results of its research and original works to the industry through its partnership with Access Control & Security Systems. The council uses professional staff and a distinguished faculty of former CSOs and content experts to develop these services and products. For more information about the council, visit www.SecurityExecutiveCouncil.com/?sourceCode=access