SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

Benchmarking Guidance for CSOs

ASIS

Originally Published in Security Management

December 2008

Benchmarking Guidance for CSOs

Chief security officers seeking ways to improve their organizations' international security programs will find useful guidance in a new benchmark study sponsored by the Security Executive Council, an international membership organization for security leaders in the public and private sectors. The study, based on surveys of more than one hundred professionals at global companies, highlights factors that contribute to effective international security programs.

"There's nobody systematically collecting data on security programs," says Kathleen Kotwica, Ph.D., the Security Executive Council's executive vice president and chief knowledge strategist. "There's a little here; there's a little there," she adds. "There's no centralized place, and I can't tell you how many people—members or not—are coming to the council saying, 'I need benchmark data on fill-in-the-blank, and it isn't anywhere.'"

During an initial round of interviews with about a dozen of the council's member companies, Kotwica found that the security programs varied greatly. "They were big companies, but some were operating in very sophisticated modes, and some were operating in less sophisticated modes," she says.

To address the problem, the council conceived and launched its International Security Programs Benchmark effort to enable security leaders to measure the performance and business value of their programs by comparing them to others around the world.

The group surveyed 149 security leaders, beginning with its own members and then branching out to other colleagues whose companies have a global presence. They also partnered with ASIS International's Chief Security Officer (CSO) Roundtable to tap other senior-level security professionals.

The online survey consisted of 58 questions, about half of which asked about specific security programs. Most participants (60 percent) were from large companies with revenues over $5 billion and with more than 1,000 employees. The majority, 80 percent, reported having security responsibility for the entire organization.

Among the findings was that security leaders at companies operating internationally devote, on average, 62 percent of resources to domestic security and 38 percent to international security. A handful of respondents operate as global companies and do not distinguish between domestic and international programs.

In addition, most international security programs are governed by corporate policy (59 percent), followed by corporate guidelines (47 percent), and regulations and laws (35 percent), the study found. Most respondents cited the time investment of employees, rather than money, as the most accurate description of how they think about budget allocation.

While only council members and survey participants will receive the full analysis of the results, the council plans to release a portion of the findings to the public in three reports.
The first report was made available in September. While there are likely many variables that contribute to a successful program, the first report focused on two: the size of the company and the department to which the international security program reports.

With regard to size, the study compared practices at Fortune 500 companies (those with annual revenues between $5 billion and $40 billion) to those at Fortune 50,000 companies (those with revenues from $50 million to $4.9 billion). It found that a large majority of Fortune 500 enterprises (86 percent) had a risk oversight group that met on a regular basis, compared to only 15 percent of the Fortune 50,000 companies.

Security awareness was also more widespread in larger enterprises. Asked whether international security programs and services are well known within the organization, 69 percent of Fortune 500 companies said that they were, compared to 31 percent for Fortune 50,000 companies.

Sixty-three percent of Fortune 500 companies have formal programs to protect intellectual property, while only 37 percent of Fortune 50,000 have the same. The percentages are similar for formal brand, reputation, and trademark programs—63 percent versus 36 percent. One question the council plans to examine through research is whether, or to what extent,

improved protections at large companies cause criminals to target smaller companies, Kotwica says.

With regard to reporting structure, the study found that respondents reported mostly to one of three groups: executive, human resources, or legal. The majority of participants who reported to executive and legal had a more sophisticated level of operations, which included being responsible for specific areas of risk and being aligned with the business side. Most of those reporting to human resources said they were more involved with policy, guidance, and controls.

Marene Allison, vice president of global security for Medco Health Solutions, Inc., and a member of the CSO Roundtable, says the survey was worthwhile. “It was good as a benchmarking study on where people spend their money for their operations overseas or in North America,” says Allison, whose biggest security concern is protecting customer data. Medco, a pharmacy benefit manager in the Fortune 50,000 range, conducts about 5 percent of its business overseas.

Another plus regarding this study is that much of the information is being shared free. The three summary reports will be available on the council’s Web site as they are released.

Security leaders can use the findings to see what kinds of formal and informal programs different companies have in place and to assess whether similar programs might work for them.

About the Security Executive Council

We are a research and advisory firm for security leaders. 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 Stakeholders). Tier 1 Stakeholders 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 seeking 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 at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com