SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

"Garbage In" Can Cost You Your Job

Bob Hayes and Kathleen Kotwica

Originally Published in Security Magazine

We recently conducted a poll on our Web site asking visitors the question, "What in your organization is putting your continued employment at greatest risk?" Eighteen percent of respondents said lack of leadership buy-in or support; 16 percent said inability to demonstrate value; and 11 percent cited security program failures.

As we looked at the poll results, it struck us that these three issues, which account for nearly half of the total responses, can all be caused at least in part by bad information. Garbage in, garbage out. If you don't start with high-quality ingredients, you're not going to get high-quality results.

It's easiest to see how basing your security and risk decisions on inaccurate or vague information can cause security program failures – perhaps you put a low priority on a certain threat based on bad information and that threat turns out to be imminent and of great impact. Lack of buy-in can happen in a similar way. For instance, what if you use uncorroborated or incomplete data to support a program proposal and your boss asks for finer details that you don't have and can't get? Would that not result in a severe drop in management confidence? Last, if you base program decisions on the wrong information, you could hinder the security function's ability to create and demonstrate value. If you implement a security program simply because it seems to have created value for another organization, for example, but you don't understand the factors that differentiate that organization from yours, that program decision could easily backfire.

The sad part about this is, 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.

- **Personal opinion**. There's something to be said for going with your gut, but the pitfalls of relying on opinion alone are obvious. Even if your opinion agrees with that of your peers, without some stronger corroboration you cannot con- sider yourself informed. Plus,

management will have limited confidence in your methodology.

- **Ad hoc benchmarking**. Benchmarking varies in its effectiveness. Rigorous benchmarking, when done effectively, can provide a limited snapshot of common sector or cross- sector practices that can help influence your decision making. Unfortunately, benchmarking is rarely done this way. Usually it is self-reported data provided by whoever happens to answer the call. This may be simply the person who has time to respond to the benchmarking request, not the per- son who's most knowledgeable or who has the most relevant programs.
- **Selective and vetted benchmarking**. This type of information is supplied by people and companies who are selected by a knowledgeable source because they have been shown effective or successful. It is a group of known elements who are able to elaborate on their situations and decisions in order to better inform others.
- **Research**. Research applies rigorous procedure and study to issues. This includes a carefully selected pool of a set mini- mum of representative respondents, in some cases supplying redundant lines of questions to ascertain reliability, following up on questionable answers, removing outliers and often repeating benchmarks for trending purposes. It may include both qualitative and quantitative techniques.

One problem with the security industry today is that the majority of our information is coming from the first two categories in this list. We're inundated with incomplete and inaccurate information.

You need more than numbers and yes/no answers to deter- mine whether most data from or about other organizations' practices is applicable to your situation. Based on more than five years of research, we have determined that an organization's culture and "acceptance level" for risk reduction pro- grams, the security leader's leadership capabilities, and the program's maturity all deeply impact the success potential for rolling out new and enhancing current programs. If you don't understand how these elements factor into the information you're getting from other organizations or sources, then that information could be useless to you, damaging to your cause, or devastating to your career.

It is time for security to go beyond haphazard information gathering. It is time for us to join other business functions in developing sources of research and core knowledge that can be called upon to provide valid, reliable and complete data that more accurately explains or enhances the multi-faceted reality of our function.

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 here: https://www.securityexecutivecouncil.com