SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Measuring the Business Value of Security

Geoff Kohl

Originally Published in SecurityInfoWatch.com

August 2007

Measuring the Business Value of Security

The Security Executive Council weighs in on why security metrics are important to your job

The Security Executive Council (SEC) recently completed an online survey which queried respondents on how they used metrics (the survey also reviewed workplace violence). While the full research is not public (SEC members have access, as well as those who participated in the survey), the Council did note that they found that only 31 percent of the respondents "gather security program data in order to create statistical reports to present to senior management." Conversely, the council notes that all of its members report that they use such data in their reports.

Faced with such an alarming statistic (and the disparity between SEC members and the general security public), SecurityInfoWatch.com caught up with Security Executive Council's Bob Hayes and Kathleen Kotwica to shed some light on what it means to report security metrics.

SecurityInfoWatch: Should this 31 percent statistic be a wake-up call to security managers to start collecting data?

SEC: Yes, it should be more than a wake-up call that 67 percent said they don't collect information -- it should be an alarm. When you look beyond the statistics to see what people reported as the reasons for not collecting data, you see that a large percentage didn't collect data because management hadn't asked for it. That should be an alarm to security managers, because it may mean management isn't even aware that security has metrics that may impact the business, or it may mean that security is being left out of the mainstream of the organization. Respondent comments also indicated that some security managers don't know what metrics are or how they should gather or report metrics, and that will require some training and education. And some of the responses seemed to show that other security managers feel that collecting metrics is more work than they want to do, and that is definitely a wake-up call. If your management has an interest or develops an interest in this area, you'd better be ready to respond.

Additionally, should businesses without a dedicated security department (or those that might simply hire out "security" to a guard services company) be collecting this data?

Absolutely. It's actually even more important if you're contracting, because you're placing really high risk in other people's hands. You have to evaluate how well they're doing and how effectively you have to have a way to quantify it.

If there's no dedicated security department because the company is small, keep in mind that it's the small companies which can't afford incidents. Large incidents are often the cause of companies going out of business, whether it's a large fire or a natural event or a business continuity problem. Small companies should be able to glean from the metrics the value or the risk to the corporation how much risk they have and how much they're accepting. Small businesses especially should be doing this.

Outsourcing is an issue for large corporations as well, and metrics are also necessary there. One SEC member for a very large corporation outsources his security 100 percent and he uses metrics extensively, because he has to know how security is doing, whether it's in house or not.

Are there legal/liability issues that arise if a company collects (or doesn't collect/report) security data?

A lot of security regulations require some form of measurement showing how the regulation is being implemented and how effective it is, and that's an issue if they don't collect data.

From a liability standpoint, security data doesn't really change the equation if there's a wrongful death suit or something along that line. Whatever data you have can be subpoenaed if you have a legitimate suit. But a good metrics program presents that data in a way that's beneficial to the company and shows a level of professionalism that often defends the company. In fact, it should be your best defense if it the metrics you've shown are well managed. If you have great metrics but negligent management of those metrics; that is, if the metrics are showing that crime is skyrocketing and you're dong nothing about it, metrics aren't going to save you.

Is there fear among some corporate security managers that showing their numbers might not impress business management?

Absolutely. As soon as you show management numbers, their response is, "Are these numbers good or bad? One common problem security managers have had is that they can't always answer that question with certainty. That's the whole purpose of our International Security Research Database - it gives security a way to benchmark and compare their numbers to those of other companies.

What management really wants to know from metrics is if they're spending too much or too little. If your numbers are way too low, you might be spending too much for an acceptable level of risk. If your numbers are way worse than everybody else's, then maybe you need to spend more money. Management wants those metrics because they will help them manage resources, human and capital.

So yes, there is a natural fear on the part of practitioners to say, "What if my numbers are worse than everybody else's?" but that can be an opportunity. Maybe management hasn't given you enough money and resources to impact the numbers effectively. Good metrics will always be your friend.

George Campbell, an SEC emeritus faculty who wrote the book Measures and Metrics in Corporate Security, points out in his book that management is going to measure you somehow, one way or another. If you don't have your own numbers based on the reality of the security department, you're going to have to face risk evaluated in a less informed way. That could get you in more hot water than showing your own numbers, whether they're high or low.

In terms of taking statistics to senior management to prove the value of security, what are some common measures that SEC members often use? Management generally asks for metrics in the format of dashboards and scorecards. The topics the metrics cover depend on what security is reporting on. Management is always interested in cost; they're interested in unmitigated risk and in anything that can impact the corporation in a significant way that might be regulatory noncompliance, for instance.

In terms of providing data/statistics to senior management, should it be more than just security system data (number of alarms detected; number of doors held open, number of background checks completed)?

Those data points you mention are activities, and there's a difference between activities and metrics. Activities are things like number of alarms, number of doors held open metrics show what difference it makes that we've taken or not taken certain action to deal with that. Management may be interested in how busy you are or how many cases one investigator can manage, etc., but mostly they want to know what impact this is having on board-level risk and the things that are most critical to the company. And with metrics we can make that case. We can show what role security plays as it ties to board-level risk. The council has actually recently done a research project and developed a graphic model to show how security ties into board-level risk.

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