What's State-of-the-Art in Security Metrics?

By George Campbell, Emeritus Faculty, Security Executive Council

File this in the opinion folder. I have always pinned my metrics hunt to that day very early in my CSO career when the boss asked what kind of metrics we had in the can. As I stumbled for a defensible answer, he said, "I want you to think about what metrics we should follow in our organization and why you think they are important for the senior management team." But the more I dig into this security space, the more I have found that measuring and plotting program performance has been an expectation of every boss I've worked for over these past (gulp!) 50-plus years.

Why then is there such a vast wasteland of security metrics available to us for our disparate security operations? Google "security metrics" and you will find page after page of solid, established results...on information security. Dig for the rest of the content we loosely label "corporate security" and then try to dig some more. It is not surprising — the crown jewels are virtual, moving at the speed of whatever from wherever to somewhere out there. Management's perception of risk has expanded almost as fast as the intelligence of the evil propeller heads who know how to find those jewels. If you were to ask the average CEO what security concerns keep him awake at night, you would likely get something about information protection. Our information security colleagues have done an outstanding job of understanding their universe of risk, developing detection and prevention tools, and building a body of standards and measures of security program performance. Why have we not followed suit?

Contract security guards in the United States alone account for more than $16 billion and employ significantly more people than public law enforcement. Businesses spend billions on physical and logical security technology and tens of millions on background checks and an array of investigations. Yet, when you ask a source that should know what the total cost of security is in their company, they typically don't know the answer because there are too

many variables spread across multiple parts of the business.

Given the expanse of the larger corporate security universe, where are the established standards, measures, metrics and benchmarks to guide comparison and program performance assessment? Why did ASIS struggle for so long before uttering the word "standard"? If NFPA and OSHA can issue codified standards on workplace safety, where are the statistics we can use to assess how we stand vs. industry peers in workplace violence and other key risk areas? How do my security program costs compare to others by revenue, sales or size? How about a measure of ethical health like the ratio of employees as subjects of investigation per 100 employees? I've got a few hundred of these, but so would you if you really thought about it.

Why is this important anyway? I think there are several reasons, but here are a few:

1. Because if you're not measuring, you're not managing.
2. You are in the risk management business. What impact are your security expenses having on your exposure to risk? Is your organization safer and more secure than it was at this time last year? How are you measuring that, and what have the adjustments accomplished?
3. Management gets metrics from just about everybody else in the company. What are they to think if you aren't advertising your performance metrics?
4. Your organization's level of security depends on non-security staff to engage in a variety of actions to protect your assets. How are you measuring their performance?

If you need a more help creating a security metrics program, there is a 40-minute presentation available for purchase: Building a Security Measures and Metrics Program, 1st Edition

Originally Published in CSO Magazine

Visit the Security Executive Council web site to read other articles in the How to Get Started with Security Metrics 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 here: https://www.securityexecutivecouncil.com/