Key Performance Indicators: How are you Evaluating your Security Program?

PINKERTON®

Are you relying on compliance with a service agreement, daily communication, and relationships to measure the effectiveness of your security team? If so, take heed. "There's a push in the security world to look at key performance indicators in order to get a more objective measure of a security program's performance," says Jack Zahran, President of Pinkerton.

In today's market, it's not enough that your security program is in compliance with the service agreement you have with your vendor. In addition, just knowing reported activities, time and money expended isn't enough to measure true results or analyze areas of weakness. Key performance indicators, or KPIs, have long been a way for corporations to measure the effectiveness of specific programs.

However, the security field, along with many other industries, relied on the adage, "If it's not broken, don't fix it." Of course, under that premise, you only know your program is "broken" when disaster strikes. That's why using KPIs is becoming a solid way for companies to analyze security programs on a more personalized level. Obviously, not all companies have the same needs. A nursing home will have very different security needs than a petrochemical manufacturer.

In addition, KPIs can also be important to clients who need to demonstrate compliance in a documented way. "Certain industries have regulations that are closely monitored. KPIs offer another tool to measure where you've been and what your goals are, as well as document compliance," he says.

But metrics are more than just numbers, cautions Zahran. Key executives must be able to put the numbers in context and interpret them in order to truly make them meaningful. And, to do that, you must be able to take the raw data and define a set of values to measure against. So, in addition to quantitative indicators, you also have indicators that examine company processes, which direction the company is going, where action can be made and the financial impact. "I suggest you have all the appropriate stakeholders involved in developing your corporate KPIs as they relate to security," says Zahran. "I would include the operational folks as well as business partners, procurement and finance."

Here are some tips for developing KPIs for your business:

Know your business. It seems so obvious, but the key to developing sound metrics is to know what's important to your business as it relates to security. You must know your current and potential risks and how your business strategy and culture impact your approach to your security program. For example, key metrics for an auto manufacturer will differ dramatically from a nursing home. "In an auto plant, response time and safety are critical, but in an office lobby environment, the factors you should consider are related to appearances, talking down a difficult person, and professionalism," says Zahran. Drilling down to the main performance objectives will help you more effectively evaluate your security program. For example, a retail store may have three goals: to protect its employees, to protect its physical assets and to protect its financial assets. Once you've identified the main areas to measure, you can develop KPIs accordingly.

Keep it manageable. Let's face it; you could list hundreds of key metrics to evaluate; however more isn't always better. According to Zahran, keep the number of KPIs that you evaluate to fewer than eight. "You don't want to be living in the detail," he says. "Boil it down to about four or five key variables." Too many will be ineffective and too few will miss key areas that need improvement.

> "Don't wait until a breach in security to figure out where your program needs work."

Develop a qualitative scale. It goes without saying that your KPIs must be quantifiable and, as such, they must be compared to another number, such as last year's budget or goals. That's why it's important to develop information that shows trends over time.

Once you know what you're looking for, it's important to take stock quarterly, semi-annually or annually to measure the effectiveness of the KPIs you choose. "I like to use a satisfaction survey that offers a seven-point scale (7=best; 1=worst). By doing this consistently with the same measurements, you build trends over time and can truly see where your strengths and weaknesses are," says Zahran. Choosing when to review your KPIs depends on the cadence of your business. If you tend to have semi-annual business goals, then a semi-annual review of KPIs makes sense.

Analyze carefully. Once you have these measurements, you can develop new measures to closely align with your key metrics. "The most important thing to consider when developing KPIs is to ensure that they support sound decision making," says Zahran. "Continuous improvement and consistency are important in developing most security programs, so the progression of the program must be in line with corporate goals and those goals aren't static," he says. "You can measure things to death, but if the metrics don't support sound decision making then you're just making charts for the sake of charts," he says.

So, your KPIs must correlate to something. For example, drilling down to the difference between turnover rate and retention rate. You may find that the numbers show an 80% turnover rate. You think you have a problem but it's misleading because you're not getting at the heart of the issue. "If you have 10 people at a facility, and you have one position that turns over eight times, it appears you have an 80% turnover rate," says Zahran. "But if you look again, it may turn out that the position turns over so frequently because it is the graveyard shift and your other positions haven't turned over. So, you actually have a 90% retention rate," he says.

Take action. The whole purpose of KPIs is to help tweak the areas of your security program that need extra attention. But, every client's threshold for action is different. The key, says Zahran, is to keep your action plans in line with your risk aversion and tolerance. For example, one false alarm in the reception area may not be cause for concern, but three false alarms in a week warrant a warning, and five false alarms in a week mean it's time to take action. "It's an ebb and flow but you must assign accountability, track improvement and then set new goals," says Zahran.

"Don't wait until a breach in security to figure out where your program needs work," he says. The bottom line is that your security force is your first line of defense and, as such, should always be operating at the highest level possible. "KPIs are tools that should be used consistently in today's dynamic security environment," says Zahran. "Determining performance in the key areas that clients deem vital will improve their core business," he says. By establishing key performance indicators to evaluate your security operations, you can effectively measure the success of your security service.

PINKERTON®

For more information, please visit our website at www.pinkerton.com or contact us
Email: pinkerton.info@pinkerton.com | Phone: +1 800-724-1616