G4S Canada
Corporate Risk Services

Whitepaper

Corporate Risk Services
Secure Integration
AMAG Technology
Security Personnel

Measuring Your Security Department

Robert Hastings

How Do We Enable the Business?

Security professionals often like to talk about security being a "business enabler". The idea is a sound one:good security helps businesses function more effectively. (And, conversely, bad security can get in the way.) But if we're not careful, this talk about "business enabler" can be just that -- empty talk, that doesn't signify anything that the people managing a business really care about.

There needs to be something to support this idea. It needs to be more than just a slogan or bumper sticker. As security professionals, we need to be able to explain how security is a business enabler, and be able to show that security programs are enabling the business to function more effectively, more efficiently and more successfully.

To do that requires using *security metrics*. When I use these words in speaking to security managers or corporate security directors, I often get one of two reactions. Sometimes, it's a blank stare. "Security metrics" may as well be ancient Greek -- it just doesn't have meaning for someone trying to manage a security program on a day-to-day basis. Other times, it's a look of sheer intimidation. "Security metrics" is meaningful, and the importance is understood, but there's a deeper worry. That they just don't know enough about security metrics to use them.

The end result is usually a quick change in topic, or an end to the conversation.

The Need for Security Metrics

In today's business environment, these reactions have to change. Every part of a business, and every business as a whole, collects, reports and manages based on business metrics. The security department is a cost centre. It generates no revenue, and produces no profit. Without valid and reliable metrics, the security department will often find itself steadily cut and cut and cut again, as the business controls costs by targeting departments that can't show their costs are justified.

Security metrics don't have to be mysterious or worrying. Security metrics are a way of collecting and analyzing evidence about the current state of the security program. This data can then be used to optimize the program against an end goal. The end goal might be controlling costs, but it could also be reducing losses, reducing the number of security incidents/reports, or improving emergency response.

There is a little bit of a danger associated with security metrics. Providing numerical measures of something -- not just a security program -- can create an aura of scientific authority. And this is there even if the numbers aren't relevant, aren't appropriate, or just aren't accurate. So, we need to be careful which metrics we use, to make sure that the business case for the security department makes sense.

Implementing Metrics

There are two key things to keep in mind when implementing security metrics. First: what is it that the security program is meant to achieve? There's a lot of different things that security could be for, depending on the nature of the business, the security risk in the surrounding environment, and the resources available for the security department.

Ideally, this is a higher-level discussion than just within the security department, involving senior or executive management within the organization. In the best-case scenario, the security department's role is mostly advisory, within a formal mandate determined by high-level management. And this purpose will be aligned with the organization's enterprise-level tolerance for risk. That is, the goal of the security department is to keep the business' risk exposure within whatever level the senior and executive management are comfortable with.

At the very least, though, the security department should have a clear idea of what its purpose is within the organization. Without this, there's no way to choose the metrics that will be most meaningful to higher-level management.

Second, how can it be shown that the goal is being achieved? If the goal is reducing losses, then key metrics will be the number and value of losses. If these numbers are decreasing over time, then the security department can demonstrate that its purpose is being achieved. If these numbers are increasing, however, then the security department can argue for improvements to the program -- which might involve more resources, better technology, or increased staffing.

Similarly, if the goal is reducing the number of reported security incidents, then key metrics will be number (and possibly severity) of reported incidents. If the numbers decrease over time, then the department is doing its job. If they are not, then the department can present a strong business case for more resources.

Getting started can be a little challenging, to be sure, particularly if the security department hasn't had a robust metrics program in place already. This is where a credentialed and experienced security consultant can be of service. Consultants who have seen and implemented many security programs, and audited or otherwise measured them, are well-positioned to provide advice and insight on the best metrics relative to the security department's overall goal.

Communication and Ongoing Management

To be effective, security metrics have to be treated as part of an ongoing process of measurement and optimization of the security program. And this has to fall within the purview of the security manager or director. What was working 6 months ago may no longer work now, as the security risk environment has changed, or the business tolerance for risk has shifted. The more relevant and accurate data that is collected, the easier it is to make adjustments to the program based on changing circumstances, and the easier it is to show the powers-that-be in the business that the changes are taking effect.

As I've already said, it also becomes much easier to defend the cost of the security department to the management of the business. Once data is collected, it can be analyzed to determine what benefits are being created for the business, and how much the business is spending to obtain those benefits.

This is the kind of information that senior and executive managers use to make financial decisions. A gut feeling that the security department is underfunded or understaffed rarely convinces the executive team. But a robust analysis based on carefully-collected metrics can prove that the department needs more resources in order to achieve its goals.

The importance of communicating metrics and analysis of those metrics can't be overstated. Regular meetings with senior managers and executives gives them visibility they need on how security dollars are being spent. It proactively makes the business case that the security department deserves its budget and other resources, and maybe deserves a little more. Without these metrics, and this ongoing process of communication, security managers are always going to fall behind other departments within the organization.

Robert Hastings, Senior Consultant, G4S Corporate Risk Services is a risk and physical security professional with 17 years of industry experience. Robert is a recognized expert in the area of using metrics to measure and drive security program success. His research into this area has been published in both professional and academic sources. Robert holds a bachelor's degree in Security Management from Davenport University in Michigan and a master's degree from Carleton University specializing in Infrastructure Protection and International Security. He is double board-certified by ASIS International in physical security and security management having earned both his PSP and CPP credentials. Robert is further certified as a Professional in Critical Infrastructure Protection (PCIP) through the Critical Infrastructure Institute.