Building a Metrics Program That Matters

The first of a two-part series from the Security Executive Council

By George Campbell and Marleah Blades

Those of us who read this magazine regularly know about security metrics. We have read about their value and seen monthly examples of useful metrics and what to do with them. But, ladies and gentlemen, we are still missing the proverbial boat. Some of us are running alongside as it pulls from the dock, waving our arms and begging it to slow down so we can figure out where the ramp is. Others are across the street at the ticket booth wondering why there are so many people in line.

In a 2007 Security Executive Council survey, nearly 70 percent of respondents stated that they do not collect security program metrics for the purposes of presenting to senior management. There is little evidence to show that the statistic has changed much since then. Sadly, the metrics boat we are missing is not just a vehicle that might take us to a cozier career life. It's where we are supposed to be, it's where our job asks us to be, and it's where our senior management should want us to be — whether they can verbalize it or not.

The survey referenced above asked respondents why they did not collect metrics, and three themes emerged among their answers:

1. Management has not shown interest or requested such information.
2. My program does not have the funding or budget to do that.
3. I would not know where to start.

This article will eliminate the third obstacle by laying out the basic steps for creating a security metrics program. But before we go there, let's quickly address obstacles 1 and 2.

Problem: Management has not requested security metrics.
Solution: Surprise them.

In one way, you are lucky. You are flying so far below the radar that they do not even know you are there. Consider this: Does your management want to be able to clearly see whether you are conforming with corporate values and policies? Would they like to have a visual representation of the state of the company's risk — desirable or undesirable? Would they like to have measurements and data at hand that show whether the company is in compliance with applicable laws and regulations? Do they want to know whether past and current security investments have resulted in decreased risk or fewer incidents, so they can more easily determine the direction of future investment?

You can provide all this with security metrics. If management is not asking for them, the best-case scenario is that they do not realize that metrics are the way to get these results.

The worst-case scenario is that either they do not consider Security an important part of the business, or they do not know what Security does. They are asking for metrics from nearly every other business unit. If they are not asking you, it might be because they are not thinking about you at all. If that is the case, you have big problems.

But when it all comes down, it does not matter why management is not asking us for metrics. We should be providing them. As the security experts, it is our job to manage risk and to inform management on our status. We should be taking metrics to them — we should not have to wait to be asked.

Problem: We do not have the money to create a security metrics program.
Solution: What money?

Measuring your various programs is not something extra to do. It is a key element of management and an expectation of your position. Metrics are the outputs of the measuring process. The tools and data you need to create security metrics already exist. If you conduct after-action reviews, if you speak to your peers about trends and best practices, if you assess your risk on a regular basis, if you track project status or log incidents, you already have the necessary data. If you have access to a computer with PowerPoint, you already have the necessary tools and technology. Do you need to do some analysis to turn this data into metrics? Of course. You might not have the budget to dedicate a staff member to metrics creation, but who better to develop the necessary metrics than you? You know the program, the business, the risk, the needs, and you have the authority to collect and access all the information you need.

And again, if we as security professionals are not doing what we can to ensure that management is informed of business risk and how we are addressing it, we are not meeting the obligations of our position. If building metrics means we have to put in more time, then as difficult as it may be, every security manager at every level should put in that time.

With those objections behind us, let's consider five steps in building a responsive security metrics program.

Step 1: Identify the business drivers and objectives for the security metrics program.

A security metrics program is as important for the business as for Security. As discussed, security metrics can provide all kinds of results that senior management would appreciate, such as evidence of regulatory compliance and assessment of security program investments. Before you set out building your program, consider your business' goals, needs, values and policies. Think about the specific results metrics could provide and how they match your company's objectives. Focus on creating a metrics program that responds to the primary concerns of your business.

Then, lay out the objectives of your metrics program. Do you wish to use metrics to make a positive impact on company policy and culture? To impact risk exposure? To demonstrate Security's alignment with business

goals? To demonstrate cost effectiveness and the value of Security? Be clear on your priorities and objectives as you begin to develop your program, and record them in writing as a resource for the future.

Do not take this step lightly. Create a formal process for identifying what management wants and needs, and communicate to them Security's role in their vision. There is a clear correlation between how well you identify these needs and how successful your program will be.

Step 2: Determine who your metrics are intended to inform and influence.

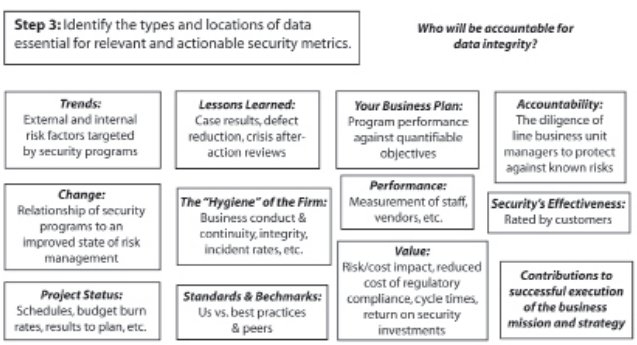
Chances are, as you begin to create security metrics, you will find that different metrics address different business units and different levels of the management hierarchy. For example, a metric that demonstrates a business unit's inaction to correct a known, reported vulnerability could be presented to the business unit manager (to encourage them to correct the issue) or to an internal audit committee (to preemptively show that Security reported the problem for correction). Each of these audiences has a unique agenda and set of needs, and the presentation of the metric should be tailored to speak to the needs of the given audience. It might be helpful to create a list of all potential audiences and their primary business goals, which you can use as both a reminder and a reference as you create individual metrics.

Regardless, metrics should be presented as enabling tools rather than criticisms whenever possible. They will more likely result in positive action if the audience feels he or she is being given an opportunity rather than a tongue-lashing.

Step 3: Identify the types and locations of data essential for actionable security metrics.

Actionable metrics require analysis, draw conclusions and tell a story. The results they demonstrate provide direction for decisions, affirm actions taken, or provide clarity for next steps. Non-actionable metrics simply count things and have little value for influencing or finding causes of risk.

Take a look at the business drivers and objectives you outlined in step one, and then consider the types of data you might need in order to create meaningful metrics that help meet those objectives. Have your programs resulted in an improved state of risk management? How, by how much and why? What was learned that should modify business process and thereby eliminate future risk? You have a staggering amount of data in the files associated with your service portfolio. You have invested financial, personnel and technology resources into



understanding, preventing and responding to the risks on your watch. What have these investments accomplished?

Step 4: Establish relevant metrics.

Relevant metrics clearly link to something you want to accomplish that has a direct benefit to the business. We can approach this step in a couple of ways:

1. Establishing metrics that demonstrate our role in enterprise risk management; and

2. Establishing metrics that demonstrate our alignment with business strategy and objectives.

4A) Risk-related metrics. Risk-related metrics enable you to determine and to demonstrate to management how Security programs and services are impacting the risk to the business. To develop these:

1. Prioritize the risks confronting your enterprise. Which are most important to the business, and which have the greatest potential negative impact?

2. Determine which risks Security has full or partial responsibility for managing (remember that these may be assigned to any business unit).

3. Inventory the products and services you have in place to address these risks.

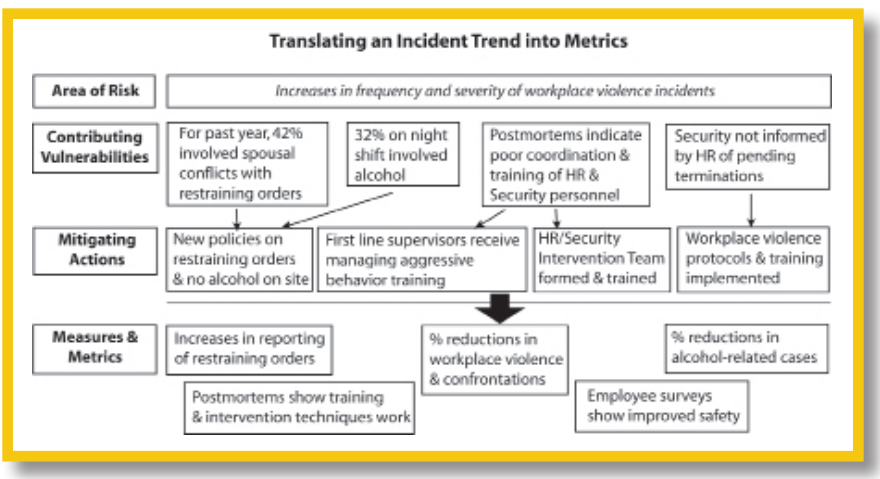
4. Identify the results management wants to see from its investment in these products or services; how these products and services are impacting risk management (positively or negatively); and whether they are doing the job reliably and cost-effectively.

These four steps will help you narrow your focus to develop metrics that matter to the business and that can demonstrate meaningful results you can use. In step 4, you will be pulling from the data you just identified to make your metrics.

The graphic on this page offers one example of how a risk that is identified as high priority can be combined with data to create an effective metric.

4B) Metrics that show Security's business alignment and value. Can you envision a metric that demonstrates the results of the steps are you taking to reduce or manage program costs while maintaining or improving the state of security in your company? For example, do we not have a value story to tell if we have significantly reduced hours of costly guard post coverage by installing technology? If our safeguards measurably remove a vulnerability that could impact brand reputation and compromise customer confidence in our products or services, do we not provide a value to our shareholders while contributing to customer satisfaction? When our benchmarking demonstrates that a service we provide is delivered at lower cost than that of our competition, isn't this a value metric understood by top management?

As you establish your metrics, focus on developing ones that could serve the dual purposes of assessing risk and demonstrating value. Highlight metrics that show such benefits as increased protection and decreased cost, enhanced customer satisfaction or confidence due to security measures, increased recovery of losses, reduced risk to revenue-generating activities, reduced insurance costs, reduced risk of attack, and reduced notable audit findings attributable to security defects.



Step 5: Establish internal controls to ensure integrity of data and data assessments, and to protect confidentiality.

Without data integrity, your metrics will be useless. In this case, data integrity means more than basic information security. It also encompasses ensuring that data is reliable, accurate and appropriately managed. There are several levels of internal controls necessary.

- **Ensure accountability.** Someone must be responsible and accountable for data integrity.
- **Ensure integrity.** Make sure the content of reports, logs, incident and investigation reports and other sources is accurate and verifiable. These sources must be competently prepared and reviewed.
- **Manage data appropriately.** Ideally, data should be stored in a way that enables searching, analysis and enterprise-wide data entry from approved sources.
- **Keep it relevant.** Maintain a process of data analysis and assessment that enables you to reach timely conclusions that matter to the core needs of the business.
- **Ensure data security.** Store data and metrics securely in a manner that is appropriate to the sensitivity of the data, and maintain a process for labeling and handling of metrics.

If You Are Not Measuring, You Are Not Managing

Security metrics is not rocket science. Our IT security colleagues do it, so we can use their business performance measures and metrics to guide our resource allocation plans and enable reliable assessment of their impact. When we apply intelligence and discipline to their analysis and reporting, we positively influence enterprise protection and contribute directly to corporate health and profitability.

It is important for us as individual business leaders to develop metrics programs in our organizations, not just because it is good for business and security, but because outside forces may be stepping in to strongly recommend that we do. Next month we will take a look at public- and private-sector security metrics initiatives and what they may mean for you. ▮

George Campbell is emeritus faculty of the Security Executive Council, former CSO of Fidelity Investments, and the preeminent expert in the field of security-related metrics. His book, Measures and Metrics in Corporate Security, includes 375 metrics examples in thirteen categories that Mr. Campbell has compiled from his 30 years of experience.

Marleah Blades is senior editor for the Security Executive Council (SEC). Prior to joining the SEC she served for six years as managing editor of Security Technology & Design magazine.