SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Security Metrics > Getting Started with Security Metrics >

A Guide for Building Your Corporate Security Metrics Program

A Short Primer for Security Managers

Created by George Campbell, Security Executive Council Emeritus Faculty

INTRODUCTION

Over the past decade, my SEC colleagues and I have worked with hundreds of corporate security executives and managers who have either discovered or have been told they need to have a set of performance measures and metrics for their programs. These epiphanies or directives come in a variety of wrappers. Here are a few that summarize the frame of reference for beginning the metrics journey:

- "My new boss is asking for our key performance indicators and I'm not sure where to start."
- "We're under pressure to show where Security contributes to the bottom line and add value."
- "We have been delivering our numbers but they don't seem to have any impact with our stakeholders."

"Where to start" is the issue for all three of these managers. Regardless of the composition of their corporate security program, they all have been generating reams of data 24/7 but have neither organized nor focused the data on the stories it can tell. They have been counting activities but haven't been measuring performance value. This short guide will set forth a set of steps that security managers should use in building a basic metrics program.

Consider this: You can't manage well without measuring well.

ASSUMPTIONS

Let's begin with a few assumptions that may serve as key success factors:

- **You have an incident reporting system or framework for collective capture of reported event data.** "Collective capture" means that the full scope of your program's service offerings may be routinely tallied in a common database (like Excel) on demand.

  Why? This is where the data, the fuel for the metrics, live. Multiple unconnected repositories or sources may present a variety of barriers to accessibility and reliability and can be very labor-intensive to collate.

- **You have the scope of authority to set the rules for metrics maintenance and reporting.**

  Why? Clarity in metrics administration and program integrity are critical from end to end. If you don't have the authority but are the designated metrics manager, get the accountability clearly assigned.

- **You can identify a member of the corporate senior management team to serve as a metrics mentor.**

  Why? The CFO or somebody in your company is likely already doing metrics well and knows what it takes to make it work in your culture and business environment. Reach out and learn.

- **You can identify an individual on your team with good analytical skills and hands-on knowledge of the tools the company utilizes for data management.**

  Why? You have a full-time day job, and a good metrics program takes time and consistent focus. You will have several staff with solid computer skills and the desire to grow, or there will be an Analyst somewhere in the company that can help you jump-start to tools and processes.

- **You have engaged the Security team and they understand this is a part of the way we will manage and they have a key role in metrics success.**

  Why? Management is committed to metrics and expects results. It takes committed time and dedicated work to honestly measure how well your Security programs are delivering planned results.

- **Your Security programs can identify a body of accepted policies and performance standards to serve as guides for metrics development.**

  Why? Policies, standards and their related goals provide anchors and content for performance targeting. There are well-established best practices and benchmarks in your industry, in professional practice guidance, in applicable regulatory regimes or in industry literature.

CONSIDERATIONS

We have seen the factors listed below add up to the difference between success and failure of a security metrics program. Everyone who has a role to play needs to believe this is a part of how Security will be managed going forward. Consider each one in the unique context of your organization and then go start your metrics initiative.

Why do you need security metrics program?
You need to have a solid rationale for building security metrics. Where we've seen real success from Chief Security Officers in this space, there were a few inter-related motives driving their journey:

1) They believed in what metrics could do for the incremental improvement of their programs

2) They wanted to be able to better tell (sell?) Security's value story

3) They had a vision for how good metrics could better connect them to their stakeholders and the business. You need to believe that some good metrics from your organization and for your employer will deliver similar benefits.

If you don't know why you need metrics, I'd advise putting this more serious journey aside until you reach this state.

Who are the customers for your metrics?
Who are your customers? What do your key stakeholders really need to know from your metrics? What metrics could engage their more informed participation in enterprise risk protection and enable their success? You have a diverse array of internal stakeholders who need to hear and see the metrics that are meaningful to them. *Ask them**!*** Good, customer-focused metrics are central to our ability to influence and engage our customers in their role in corporate security and brand protection.

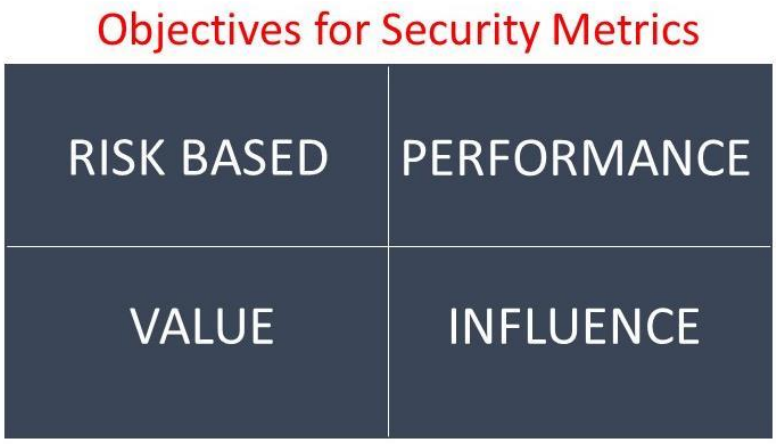
Metrics are a key part of your communication strategy. They contribute to a coherent set of messages focused on a targeted audience. You cannot over-emphasize the importance of understanding the diversity of perceptions about risk and how each of your constituents view your role in its management.

Good metrics are SMART
Specific to what is required and understandable,
Measurable from available data,
Actionable/Achievable - driving change and positive results,
Relevant to what is important and
Timely because *verifiably reliable* data is there when you need it.

You can't manage well without measuring well. Be SMART. Don't waste time building a metric unless there is a solid reason for what you want it to achieve. Remember that what we want to measure is the focus of the process; the metrics are the outputs of the process.

OBJECTIVES FOR METRICS

Your initial objective in building a basic metrics program must be to find the metrics that really resonate for your program. In our corporate security realm, I see risk, program performance, value and influence providing mutually supportive boxes in a metrics four-square. Here is a brief discussion on each of these.



1. Risk is first. (The notions of threat, asset attractiveness, asset criticality, severity and consequences are all embedded in this concept.) How does Corporate Security fit in your company's Enterprise Risk Management (ERM) strategy? What is senior management's appetite for risk and how are you influencing their knowledge of risk?

Risk is why you have a job. Security tasks are delivering data 24/7 on a variety of the more likely areas of risk exposure, and that data needs to be harvested and converted to action.

It's essential that you use a focused risk assessment to identify gaps in protection and track the various incident types that represent specific concerns for your business and stakeholders. These are the *key risk indicators* (KRI) that can provide information on emerging risks and facilitate your measurement of the results of your initiatives to attack the root causes of risk events. Each of these initiatives will have one or more *key performance indicators* (KPI) that establish specific quantitative and/or qualitative measurements on how well it has met its objective. Note that Boards and management highly value what KPIs and KRIs bring to their overview of operations and performance.

What metrics for risk?

- Assessment and inspection results: Risk assessment is a fundamental element of security management, and the results can provide clearly actionable and relevant information.
- Red flags: Highlight those risks that are the result of poor business practices and contribute to an increased probability of loss. Also highlight the vulnerabilities found in assessments and inspections. Sloppy security invites future risk. Use metrics as red flags for management attention.
- Trends: Identify business units/locations that evince statistically notable high and low trends for specific types of risk. This will enable you to then investigate the reasons for their risk trends.
- Root causes: Connect the dots across incident types so that common root causes might demonstrate how a few common mitigation alternatives can be applied for cost efficiency and impact.
- Key risk indicators: These should be monitored by appropriate Security managers and included in monthly reviews.

We own unique information on risk and how well the accountable parties (including us) are managing it. Focus on measuring root causes and the Specific actions that will get impactful results.

*Remember that what we want to **measure** is the focus of the process; the **metrics** are the outputs of the process.*

2. Program performance is second. How is success defined in your company? How well are Security programs performing, and why does it make a difference in your organization? You own a budgeted set of plans and programs with direct, measurable connections to objectives and results. Your metrics should show Security's effectiveness

in 1) delivering planned results on budget, 2) detecting, preventing and responding to targeted risks, 3) influencing business strategy and 4) delivering real value to stakeholders.

What metrics for program performance?

- Highlight the results of initiatives that target specific risks and program improvements.
- Percent of customer satisfaction scores above target.
- Metrics for contractor service-level agreement results and departmental budget and goal status should be reported monthly, with noted remediation for anomalies.
- Highlight metrics that demonstrate a verifiable return on security investment (RoSI).
- Track critical security process cycle times, budget burn and milestone progress for initiatives.

Are your key risks clearly linked to programs to mitigate them? Do all your programs have key performance measures (KPIs) assigned to their respective managers?

3. Value is next. How is value defined in your company? There are established measures across the business that should help frame a value proposition for the Security organization. Since it's generally accepted that value is measured by the benefits received, what measurable benefits are security programs delivering? What is the business case for your security organization, and what measures are baked in to the specific objectives and deliverables of this strategy? Where and how do you propose to enable the business and contribute to the bottom line? The evidence of value is in your data. But if you warehouse the data and just occasionally access it to count transactions, incidents, cases and tasks, you are not digging deep enough to identify the value-based results that Security programs are delivering 24/7.

If risk is why you have a job, how are you directing your resources to enable the *avoidance of targeted risks*? (Your business continuity team has estimates for the cost of risk and targeted recovery thresholds. If Security's response directly contributes to eliminating a known cause of risk or providing measures that directly enable a reduced impact, you have delivered avoidance.) A risk that has *successfully* been targeted for reduction or elimination provides an extraordinarily high measure of value and return on security investment (RoSI). This needs to be a key focal point for your metrics.

What metrics for the value proposition?

- Confirmed ability to contribute to life/safety
- Timely, qualitative response that directly reduces the impact of an event
- Reduction in Security cost as a percent of revenue
- Reduction in direct cost of security incidents attributable to targeted initiatives
- Reduced impact of security process on business productivity
- Identification and elimination of factors that drive cost of compliance or contribute to the risk of regulatory sanction

You have the data that will tell Security's value story. Note that reduction is a benefit. Look at the unique services you offer and how they enable business processes or how they increase perceived value for your customers.

4. Influence is last (but not least). The ability to positively influence people, policy and action must be a core competency of a Security manager. Your metrics can provide a powerful script to help you influence awareness and action. When we use our metrics as part of a broader communication strategy, we can engage management in a shared approach to eliminating risky business practices.

One of the key requirements of an effective security metric is that it is *actionable*. It needs to provide a storyline that underscores accountability and clearly advocates corrective actions. You will find good opportunities for influence in leading indicators. For example, does your data show multiple consecutive months of untested business continuity plans or increased frequency and severity of preventable security infractions in business unit X? Might a couple of metrics supporting these findings be incentives to action?

What metrics for influencing stakeholder action?

- Proposed budget reductions avoided/reversed by evidence in submitted value metrics.
- Percent of risk assessment recommendation accepted and tested as effective.
- Post awareness initiative percent reduction in incidents attributable to lack of awareness.
- Number of security policies endorsed and advocated by management.
- Percent 3rd party relationships avoided/terminated due to proactive security risk assessment.

When Security delivers visible results and value, it enhances its ability to influence action, attitude and policy. Influence is a key performance indicator for respect and credibility.

METRICS DASHBOARDS

Metrics dashboards are the metric outputs I'm most frequently asked to help our clients develop. A dashboard consolidates and aggregates relevant reporting data in a visual format for a targeted audience. The key here is the audience and time. If you are presenting, it's essential that you manage your time and focus on what they really need to know and what you want to hear back from them on the information presented.

There may be an established format in your company for a metrics dashboard, but since you have multiple stakeholders and multiple possibilities for messaging, I advise building a template that can be a home to whatever topics are appropriate for the various audiences you may have. Do you want a decision? Use the space to crisply frame the need and convincingly sell the solution. The layout should be a mix of short bullet items and a few graphs. For an established set of topics, I'd recommend a selection of actionable risk updates, three to five notable findings and a few timely headlines on accomplishments or progress on goals. The dashboard provides an opportunity to inform (eliminate plausible denial), engage, and influence. Target your content, be assured of its accuracy, and send your messages clearly.

If you only had one page to tell the right story to this audience, what would you include?

QUALITY AND INTEGRITY

Consider these two key objectives for our security measures and metrics: 1) materially impact exposure to specific risks and 2), positively influence action, attitude and policy. These objectives require an established and clearly communicated set of internal controls focused on the integrity of the data that is gathered, the quality of the analysis and assessment applied to that data and the assurance of data security and protection.

Imagine the potential consequences of drawing conclusions and formulating recommendations to management on inaccurate, unreliable data overseen by flawed, poorly supervised sources. Failing to embed data integrity within your metrics program will go directly to the credibility of the security program and its management.

REPORTING

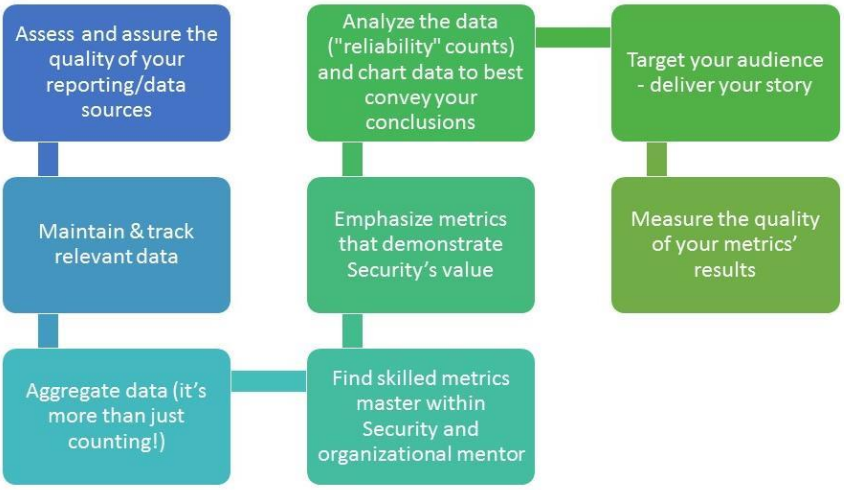
Most organizations have established requirements for the type, format and frequency of departmental reporting to include specified metrics updates that typically include one or more topical dashboards. As noted earlier, you will also need to determine the when and what of more customized metrics reports to your key customers and those you want to inform on specific findings or recommendations. It's critical to establish a monthly routine for delivery of metric reports from your program managers and contracted service providers, *and you must include an assessment of the quality of their reporting in your measurement of their performance.*

Unless you are an "army of one," you will rely on designees to deliver high-quality metric reporting based upon reliable data and conclusions. What measures of quality assurance are in place to give you confidence in the results that you must have?

CONCLUSION

Corporate security owns a unique database of business performance measures and metrics. Collectively they enable and support a key value proposition: the ability to positively influence enterprise protection, corporate policy and behavior. Enterprise protection is measurable, as are the benefits that accrue to our diverse protection programs. A well-defined security metrics program demonstrates to management how we are probing the weak spots, informing, educating, and influencing change.

As a manager, you are expected to be a good communicator. S.M.A.R.T. metrics can provide the storyboard and the script you need to for a quality connection with management and your customers.


Assess and assure the quality of your reporting/data sources
Maintain & track relevant data
Aggregate data (it's more than just counting!)
Find skilled metrics master within Security and organizational mentor
Emphasize metrics that demonstrate Security's value
Analyze the data ("reliability" counts) and chart data to best convey your conclusions
Target your audience - deliver your story
Measure the quality of your metrics' results

Visit the Security Executive Council website for other resources 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: https://www.securityexecutivecouncil.com/

