SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Security Metrics > Business Alignment >

Building Valued, Relevant Metrics Programs

Two security leaders share their experiences and advice.

Over the 18 years in which the SEC has been helping security leaders develop metrics programs, we've fielded one question myriad times: What is the most valuable metric for corporate security?

The answer is always the same: Your most valuable metric is the metric your leadership values the most.

In the SEC's October 2023 Security State of the Industry briefing, Tier 1 Security Leaders heard from two security executives who attested to the truth of that statement from their own experiences. Our first speaker, Vice President of security for a multinational brand, and Steve Slyter, CFE, Senior Director of Corporate Security and Asset Protection for United National Foods Inc. (UNFI), discussed their journeys developing and implementing meaningful metrics in their risk and security functions.

Stages in the Metrics Journey

There are five stages in the journey to meaningful metrics.

1. Define your current state and where you want to go.

2. Determine your starting point and build your roadmap. It's at this stage that you also align your plans with management's values and strategies.

3. Implement.

4. Adjust, refine, and plan the way ahead.

5. Maximize your influence.

At every stage, the process requires hard work. And, as our first speaker pointed out repeatedly during the briefing, there are no shortcuts.

Watch for Early Challenges

This security executive joined his company in 2018, when the organization was in Stage 1 or 2 of the metrics journey. His company had just begun an enterprise risk management initiative, and Security was frequently being challenged to explain how they were adding value to the company.

He wanted to be able to offer senior management a cost-benefit formula for starting or ceasing any given initiative. He also wanted his entire team to be able to explain why each security program was warranted, not only in risk terms, but in business terms. So, he began developing risk-based key performance indicators for the function.

On the call, this speaker shared some of the biggest challenges he and his team have had to overcome to move their metrics program forward.

Educating the team. Some team members had no experience with KPIs or key risk indicators. Some didn't understand what they were or how to create them. So, he carefully educated them all on both metrics and risk management – a challenging but necessary first step.

Communicating the value through KPIs. When he first brought his KPI initiative to stakeholders, it was not met with enthusiasm. Management didn't seem to understand the KPIs or the value they presented. This leader re-evaluated his metrics and their presentation and realized the problem: the KPIs he had presented were not tailored to the audience to which he was presenting. He developed different KPIs for each stakeholder – HR, Legal, Finance, the C-suite – that addressed value that was meaningful to each, and found more success.

He instituted a policy of formal, regular meetings between security team members and their general managers, rather than informal check-ins or open-door policies. Because of the increased interaction with stakeholders, corporate security managers can all now use their metrics to tell a meaningful story.

Corporate Security now sends a quarterly report that outlines KPIs and KRIs, initiatives, and

related business value for the company. They also provide an annual report in the form of a four-page slide deck that includes everything corporate executives need to focus on in small bites – the insights from the metrics that are actionable and meaningful to them. Accommodating everything in one report is difficult but critical when executives are pressed for time.

Building trust for data sharing. Our speaker learned that metrics only work if both the collector of the data and the owners of the data trust one another. Without trust, KPIs can't be established. Colleagues from other functions must trust Corporate Security to handle data carefully and wisely, and not to present it to the executive team in ways that directly reflect poorly on those functions.

Aim for Business Relevance

Steve Slyter has been with United National Foods Inc. (UNFI) for four years. Like our first speaker, Slyter found that his organization was in Stage 1 when he came on board. While metrics weren't currently collected at the company, it was clear internal stakeholders needed actionable security metrics to help them meet their own performance goals.

Slyter offered five pieces of advice that helped him build a successful metrics program.

Understand the Business. This doesn't just mean their mission and vision statement and what services or products they provide. It means all lines of business – sales, merchandizing, procurement, delivery, storage, distribution, international business, ecommerce. Understand the history and geography of the company and any potential new markets.

Learn What Metrics Are Important to Stakeholders. All KPIs must be useful in helping the business move along its desired path. And as the security team, your KPIs can also support the metrics each stakeholder is using in their own function. Sit down with the leaders of other business units. Learn what metrics they have in place and ask what might be helpful to them. Make sure to have examples ready, because they may not know what they need or what security can do.

Conduct check-ins with stakeholders at least quarterly. Make sure the metrics in place are still useful and actionable for them and keep up to date on their business strategy as it changes.

Find the Right Metrics Tool. There are a variety of systems that can help you collect and visualize the data that you need. Make sure whichever system you choose is flexible and can be modified and changed. Make sure it offers dashboards that meet your needs.

Understand the Difference Between Highlight Metrics and Actionable Metrics. Highlight metrics are counts, statistics, and amounts. These can be useful for individual audiences. Actionable metrics are more analytical. They help you find trends and root causes and take corrective actions. These are more useful to stakeholders.

Tangible Benefits

While it can take a while for any organization to successfully adapt to a metrics-driven strategy, metrics development ultimately brings tangible benefits to the organization and the security function. Gaspar noted that he has been told that his function avoided an audit by providing such useful, consistent data. And both presenters at the briefing experienced notable staff increases since coming onboard and beginning their metrics journeys – increases of four to six times the original staffing level.

The SEC has many resources available for security leaders interested in beginning or improving their metrics program, as well as metrics experts who can help guide your journey. Contact us if you are interested in setting up a conversation.

Visit the Security Executive Council web site to view more resources in the Security Metrics : Business Alignment 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/