SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Demonstrating Value > Measuring Value >

Enterprise Security Metrics: A Snapshot Assessment of Practices

Created by George Campbell, Security Executive Council Emeritus Faculty

Introduction

This 2014 report provides a snapshot assessment of the current use of metrics in corporate security management. The topic of security metrics is an obvious one for the Security Executive Council (SEC) since we have been relentless in our pursuit of enterprise-wide security metrics and performance measurement since first publishing Measures and Metrics in Corporate Security: Communicating Business Value.

In other trend or state-of-the-industry reports the SEC creates, we strive to gather information from many sources in order to examine different views, models, data sets and research output, opinions, and events. However, there is very little publicly shared information about enterprise security measures and metrics. Therefore, this report will rely mostly on the collective knowledge the SEC has amassed over the last ten years working with security practitioners at the executive level.

We have collaborated with over 100 organizations and several hundred security practitioners during this time span. We have conducted internal research, engaged in peer benchmarks, and helped build security measures and metrics programs for security leaders who see the value for their organizations. To broadcast information to others outside of our constituency, we have created books, articles, blogs, executive-level presentations, and the first-ever business case study on the topic. The information in this report is a result of this work. We hope by the second edition there will be more available information on the work others have done and shared in the field of corporate security metrics.

An Important Note on the Scope of this Assessment

This report is limited to the state of security metrics exclusive of information security metrics (InfoSec). While the collective knowledge experiences described above do include InfoSec, that area of the metrics development agenda is more than effectively documented in any number of excellent books and industry sources (see Appendix 2). This assessment summarizes our experience from these interrelated initiatives.

What is a security metric? Because there are a variety of interpretations on this definition, it may be useful to provide an established working example to set the stage.

> "At a high level, metrics are quantifiable measurements of some aspect of a system or enterprise. For an entity for which security is a meaningful concept, there are some identifiable attributes that collectively characterize the security of that entity. Further, a security metric (or combination of security metrics) is a quantitative measure of how much of that attribute the entity possesses. A security metric can be built from lower-level physical measures."[1]

[1] SSE-CMM: Systems Security Engineering Capability Maturity Model, International Systems Engineering Association (ISSEA), 2008; www.sse.cmm.org/metric/metric.asp

Put simply, security metrics are the application of standards for measuring enterprise security elements and features. There is an established business principle that says if you are not measuring you are not managing. Measurement is central to performance assessment and resource management.

Where Are We Today?

If you were to Google "security metrics" you would find page after page of solid, established results...on information security. Infrastructure reliance, IT investment and evolving threats over the past several decades have ramped up board-level perception of risk to a point that if were you were to ask the average CEO what keeps him awake at night, you would likely get something about data protection. Typically, the only mention of security in most annual 10-K statements is information protection risk. Our information security colleagues have done an outstanding job of understanding their universe of risk, developing detection and prevention tools, and building a peer-based body of standards and measures of security program performance.

The following graphic (Figure 1) displays a host of metrics-rich functions led by security's peer-level managers who understand and depend on specific measures and associated metrics. As a counterpoint, it also highlights a key obstacle to security management's greater engagement that was documented by the SEC in a 2007 survey, which included respondent practices in maintaining security metrics.

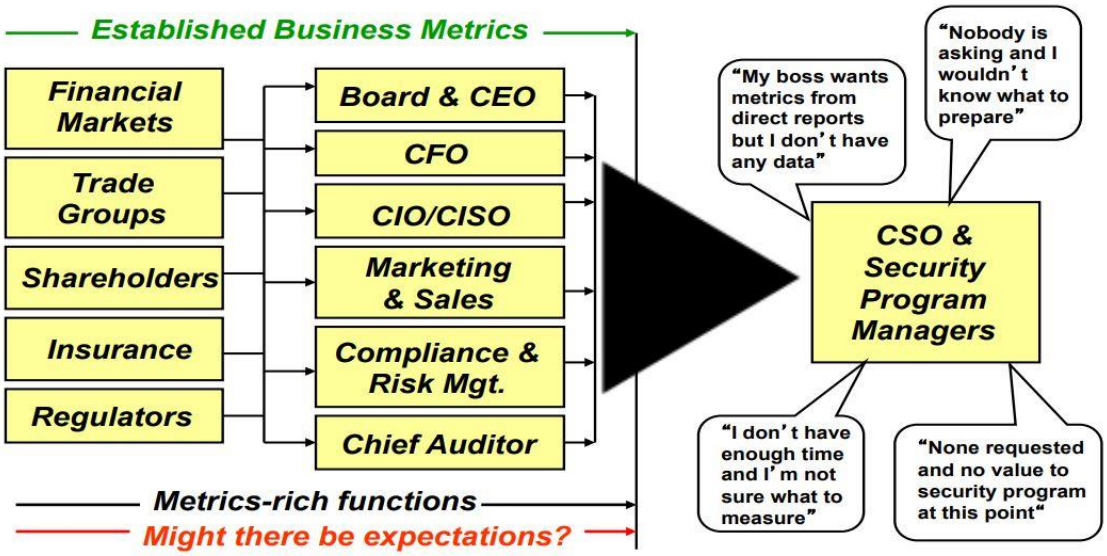

Figure 1

Nearly 70 percent of respondents stated that they don't collect security program metrics for the purposes of presenting to senior management. Respondents cited several factors for this lack of engagement, four of which are represented and highlighted in the above graphic. Seven years later, as of this writing, lack of engagement remains as a significant internal obstacle to metrics acceptance and development. Too many corporate security practitioners have either avoided or failed to understand the relevance of such measures. Security organizations have the data. They are willing to count events and other activity data, but they apparently don't see the need to use it to build actionable, influential metrics that can effectively influence senior management.

Obstacles

There are real obstacles and institutional constraints that are driving the state of the industry (and art) in security metrics.

Self-directed limitations. Our interviews with a number of security managers have found that many believe their executives don't clearly articulate what types of business-related security metrics they would like to see. However, in many instances these same security managers fail to sell their own unique perspectives on enterprise risk to influence corporate risk perspective, appetite and policy. Management needs to know whether past and current security investments have resulted in decreased risk or fewer incidents so they can more easily rationalize the direction of future investment.

Institutional barriers. There is no accepted organizational model for corporate security to drive comparability of program content and a collective view of related performance measures. While most companies may employ protective services/physical security elements, they may be proprietary, contracted or a hybrid with significantly different approaches, and the companies' geographic and service requirements are so dissimilar as to confound reliable comparison. Generally, even within specific industrial sectors, there is no established template of company requirements or security mission, risk, resource or functional commonality. Conversely, the reason IT security has the ability to develop an accepted body of measures is the commonality of threat, risk, technological orientation and mission requirements. This is also true of other administrative services like HR and Audit that tend to have a similar set of functional objectives regardless of ownership.

Different frames of reference. The lack of cohesion and structural unity dictates extremely differing perceptions of need on behalf of the leaders of these security organizations. Risk and performance measures are highly influenced by unique cultures, business strategies, management styles and business drivers. Identifying a metric as vanilla as "security cost as a percent of revenue" can be difficult if you are only comparing security-related apples to apples. Where consensus does exist, it has been

driven by industry or sector threat concerns such as those seen by data compromise events in the defense industrial base.[2]

Expanding outsourcing. There has been a measurable increase in outsourced services and downsizing of employee-based departments. The corporate security workplace is dominated by vendors, and the "Army of One" security shop is a trend that appears to have traction. Contract security guards in the U.S. alone will account for more than $24.5 billion[3] by 2016 and will employ 2.5 times what public law enforcement agencies do. Businesses spend billions on physical and logical security technology and tens of millions on contracted background checks and an array of investigations. Outsourced resources devoted to fraud risk management and identity protection have exploded in the past decade. Vendor-based services appear to result in lost opportunity for relevant metrics management.

Fractured accountability. These trends and factors add up to a fractured picture of accountability. Corporate security often may be a collection of security functions individually "owned" by HR, Internal Audit, Compliance, Supply Chain, Facilities, business units or others residing in their respective silos. Unless there is a centrally oriented structure like a Security Committee directed by the CSO, it is unlikely that the risk and resource dots will be effectively connected to provide an integrated view of risk and mitigation strategy, let alone risk and performance metrics.

Limitations in metrics scope. Too many organizations are satisfied with counting—using numbers of incidents or workload as the final step in communicating risk and performance indicators. Simple counts, when used as a security measure, can be especially hard to classify and interpret. For example, does an increase in the number of viruses detected by anti-virus software serve as a leading indicator because the increased activity indicates an elevated threat level; or does it serve as a lagging indicator because the increased activity demonstrates a highly efficient anti-virus mechanism; or does it serve as a coincident indicator because the increased activity acts as a notification that other security-enforcing mechanisms are failing?[4] More mature security organizations dig to identify root causes and embed performance measures in their programs and risk mitigation plans. Our research with practitioners has consistently confirmed that simple counts fail to provide actionable information while analysis delivers the quality of results that demonstrate competence and business process connection.

Lack of reliable data management impacts metrics development. The lack of an effective incident reporting and data management system represents a significant roadblock for many security organizations. This is a fundamental defect for which the

[2] The top 20 critical security controls for effective cyber defense are an example of consensus audit guidelines
[3] White paper on the US Contract Security Industry, Robert H. Perry Associates, 2013

[4] Directions in Security Metrics Research, Wayne Jansen, National Institute of Standards & Technology, NISTIR 7564, April, 2009; page 6

consequences go far beyond the lack of data for metrics and into the absence of a risk-responsive base of knowledge.

Difficulty in accessing "big data." Two factors combine to inhibit security practitioners' access to big data relevant to their analytical needs. On one hand, there are scores of government and private-sector databases that can serve corporate security, but they are largely unconnected and typically contain very dated information. On the other, corporate security owns a huge repository of incident data that is deemed private and is not readily sharable. Here again, the IT security sector has addressed their need for comparative data and has been able to gather highly valuable information on a wide array of risks through sector-supported surveys and reports. A variety of IT security examples may be found online. The 2013 Ponemon Institute Cost of Data Breach report is an excellent example of data that enables actionable learning on causes in this area of enterprise risk.

Limitations of individual practitioner data gathering efforts. Over the past couple of years, we have heard complaints that security practitioners find their e-mail inboxes increasingly jammed with invitations to participate in this or that group's short survey to gather data on a single topic that can then be analyzed and charted to allow participants to see where they stand among their peers. The results of these efforts can be useful for informal purposes, but they are generally not controlled enough to offer results that are appropriate for wider use. Also, these initiatives have generally been proprietary to a single organization or publication, leading to limited respondent pools and limited usefulness. Unfortunately, the security industry too often shows itself unprepared and unwilling to develop a framework to accommodate performance measurement schemes on a significant scale. This leaves practitioners on their own to seek out comparative information and quantitative measures.

While these factors clearly inhibit the growth and larger application of corporate security metrics, the SEC has used its position within the industry to more directly probe its members, groups of practitioners, leading security executives and others on their experience and needs within this security metrics discipline. An overview of those examinations is described below.

A Multi-Track Focus on Metrics State-of-the-Art

The SEC's continuing feedback from members during this early period and our more intensive review of the state-of-the-art underscored a need to probe the experience of more progressive corporate security organizations and their leadership's views on the use and utility of program measurements and metrics. To this end, we commenced a multi-track approach to 1) document current practices, 2) engage practitioners in identifying a recommended body of key risk and performance indicators, and 3) identify

opportunities to support companies seeking to assess their needs and build a responsive metrics program.

Benchmarking and Security Metrics

The SEC has utilized benchmarking fairly extensively over the past several years to both gather comparative data for our members and to identify gaps in the knowledge base that need to be addressed. Benchmarking is valuable for gathering baseline data on individual companies. It's the differences in risk, demographics and security programs among these companies that require more in-depth examination to find valid points of comparison or find ways to cull specific areas of comparability. Therefore, rather than rely upon this process alone, we have often chosen to follow up the data gathering with a peer-based approach of topical Working Groups and Best Practices Groups for drawing conclusions and identifying best practices.

The benefits of benchmarking. While it's clear that metrics developed for comprehensive security program management lead to significant internal benefits, their value can increase when they're intelligently paired with the metrics of others. Benchmarks are valuable when they bring understanding of organizational assets, risks, regulatory requirements, and a security program's "best fit" to light. This type of effective security research can lead to new value discoveries such as cost neutrality or competitive advantages perceived by clients and management alike. Comparing metrics results with the results of like-sector and cross-sector businesses facilitates rating a security program's performance, which could help to identify security gaps as well as gain funding and executive-level support. Without metrics results from other companies, you are limited in identifying what's missing from among your own security measures and programs. Your internal metrics may show that you're meeting your own and your management's standards in all your existing initiatives, but they can't tip you off that your standards are lower than the standards of 80 percent of the other companies in your sector.

Cautions on benchmarking. Benchmarking is gaining popularity and it seems particularly so in corporate security operations. But it is necessary to critically evaluate the source and content of requests to ascertain the competence of the approach and potential value of the results to be shared. This is one reason to rely on trusted colleagues as sources of benchmarking efforts. Benchmarking requests are often badly crafted, incorporating too much industry diversity, which leads to apples-to-oranges comparisons. Sometimes they're designed to support the program's current status rather than to identify a best practice, and results may fail to draw appropriate conclusions as to why company approaches to security may be different. These surveys often create more questions than answers, especially when you consider the variations in differing organizational risk environments and tolerances, asset bases and business footprints. The bottom line is that legitimate benchmarking needs to provide an appropriate level of detail in order to enable actionable conclusions.

Early metrics survey efforts. This report previously noted an early (2007) SEC member survey that documented a lack of engagement on security metrics. To probe this further with a different, more senior group, in 2008 this author surveyed 105 security executives on 13 security metric examples they would select as the most beneficial to them and their company. They were asked to rank them on a scale of 5 = most beneficial to 1 = least beneficial. The top five selections were as follows:

1. Scorecards on business risk and compliance- 86%
2. Aligning Security with business objectives- 75%
3. Dashboards for management reporting- 68%
4. Measuring cost and return on investment- 65%
5. Assessing threat and risk- 60%

It was obvious that this more senior group saw the most impactful metrics in communicating security's more fundamental connection to the business. This notion of alignment and value remains as a consistent theme in the SEC's interactions with senior security executives and serves to drive some to build far more robust metrics programs.

Probing current practices and benchmarking. In late 2009[5], the SEC intensified this security metrics exploration with a more comprehensive approach. We collaborated with twenty-seven corporate security organizations serving major global companies. The initiative began with an in-depth benchmark survey to gather information on their security mission(s) and current status of their security metrics program. We also sought to explore their desires for an expanded portfolio of measures. While this was a relatively small sample, these companies represented a solid cross-section of industry sectors and all had mature and multi-service corporate security programs, several engaging in best practice operations. The survey provided a detailed view of the status and focus of metrics initiatives in the member companies. This current state assessment was then expanded with the formation of a Security Metrics Working Group accompanied by a series of monthly sessions to examine different metrics being utilized in various corporate settings and obtaining feedback on new examples that were built for discussion.

Several highlights from the initial benchmarking exercise and these Metrics Working Group sessions are summarized here.

Who is driving the need from above? The general consensus was that the push for metrics was driven about one-third by higher corporate management, a third self-driven and a third with both as drivers. In spite of this range of prompts, about 75% of

[5] Later benchmarking and individual program review results by the author are consistent with these findings.

participants indicated that metrics was an accepted element of other business operations and this was an influence in their interest.

What business drivers are pushing the need for improved metrics from within the security organization? Some common themes emerged to provide a focus for the Metrics Working Group's efforts:

- Benchmarking program efficiency/effectiveness and security's Return on Investment (RoI).
- Improving alignment with the business and helping the business make [more] informed decisions about accepting or remediating security risks.
- Establishing required key risk indicators (KRI) and performance indicators (KPI) for various elements of the business.
- Demonstrating to senior management current state of security at each site, performance targets, and improvements in service delivery - more clearly articulating the security risk to the business at a higher, more actionable level.
- Many companies are increasingly analyst driven and data focused. As such, they have always had to use grounded data and benchmarking to demonstrate program results and effectiveness.
- Measurably demonstrating risk reduction, improving responsiveness to risk assessments and enabling improved means of communicating these factors to senior leadership.

What have been the roadblocks to metrics development? As compared to the earlier samples noted above, this mature group of large corporate security organizations expressed a strong desire to develop a solid platform of metrics but also shared frustrations on data availability and resource constraints. Our assessment going in—that there was a limited body of work in general security measures and metrics—was affirmed with broad consensus on what our members saw as the biggest roadblocks to developing the kind of metrics program they believe would be of the greatest benefit to their department:

- Lack of standardized, industry-wide metrics.
- Lack of standard metrics and techniques and the willingness to share.
- Lack of agreement on which activities and incidents measured against each other define effectiveness, the definition of the thresholds or triggers that would constitute an alert, and the multiple databases that have to be mined long hand, instead of just automatically.

- Lack of systems across the organization to capture the necessary data, staff understanding of the importance of metrics, and the lack of executive focus on security metrics (the focus is on operations).

- Not being able to get our arms around the proactive/preemptive facets of security that cannot be measured and not looking outside the security team for the total dollar impact to the company.

- Lack of time (resources to devote to metrics administration) and the lack of peer data.

- Lack of ability to obtain or develop metrics that effectively demonstrate hard benefits that justify security spending. (This is a consistent concern expressed across multiple surveys and customer interactions on security metrics.)

- Program maturity, lack of transparency and data spread out all over.

What security programs served to prioritize group members' metrics? It is not surprising that a clear majority of the SEC's 2009 survey respondents indicated multiple mission-related points of interest for their metrics program. [6] An interesting sidebar to these discussions unfolded during the later sessions as security's ability (and challenges) to align and influence their business unit clientele took on more interest and priority.

Session agendas tended to use the six topical categories seen in the program focus column in Figure 2 and various members provided high quality information on their metrics initiatives within these categories. Understandably, these contributors emerged from among the participants having more mature metrics as seen in the top two bars in the left column. It is also noted that the more experienced practitioners are from among those with an information security portfolio—another indicator of the maturity and richer inventory of data in this discipline.

[6] The chart displays higher totals due to respondent selection of multiple program interests

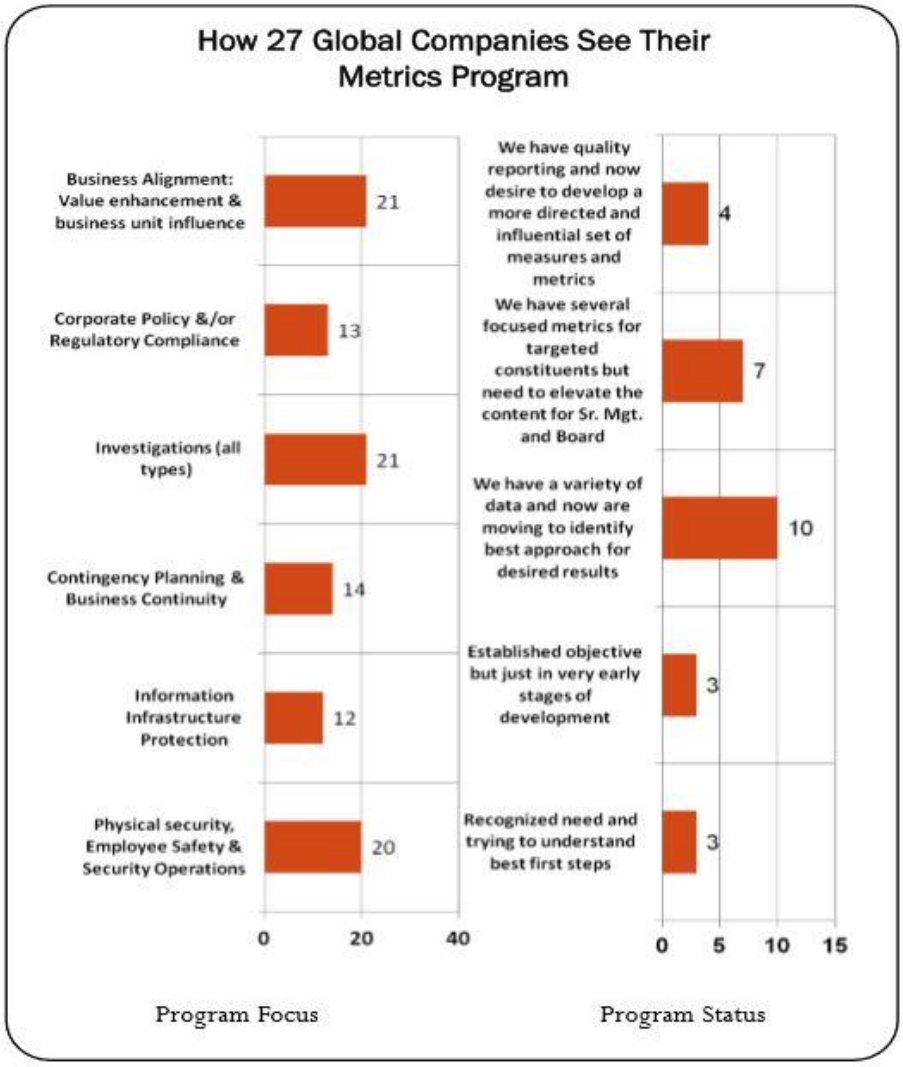

Figure 2

Summary of the Multi-Sector Exercise

This initial Working Group brought together senior security managers from high tech, manufacturing, retail, consumer products, healthcare, communications and aerospace. They were asked to identify a few security metrics that could work within their companies and support their diverse portfolio of security services. As seen in Figure 2, a positive for the results was that over 75% described a relatively mature experience with their metrics program, with the balance fairly early in their metrics evolution. Group discussion ultimately arrived at the dozen metrics seen in Figure 3. Follow-up polling focused on ranking each metric on a 1 (highest) to 5 (lowest) and, for the purposes of this discussion, only those selected in the top 2 tiers were tallied as indicated in the red and blue bars in Figure 3.

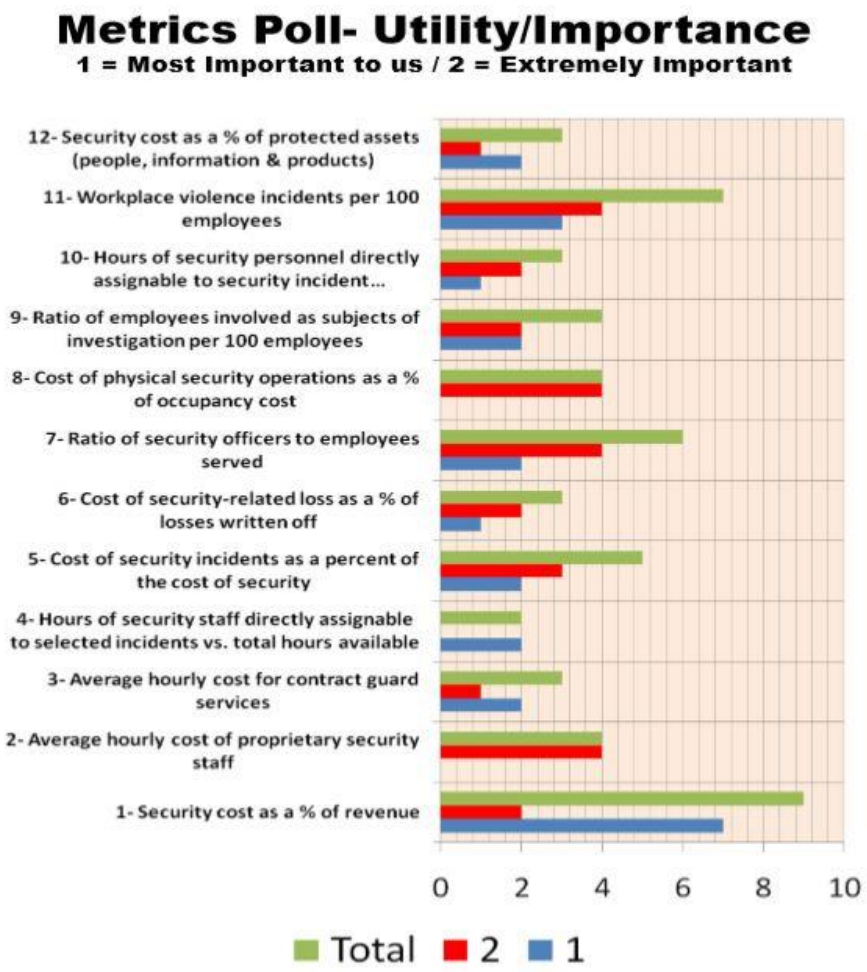

Figure 3

This group of security leaders tended to reflect a strong connection to the challenges confronting their businesses such as global expansion, cyber risk, outsourcing (the expansion of insider risk) and cost optimization. There was a consistent theme and evident need to leverage metrics to more effectively communicate security's value proposition and demonstrate the relationship of security programs to business objectives. Due to the diversity of the companies represented and the expansive service portfolio of the members, the risk portfolio evidenced fewer common risk drivers.

This benchmarking initiative demonstrated the relevance of a small but diverse set of measures to a cross-sector group of security executives. A key finding was to the universal acceptance of the need and value of security metrics to their internal management objectives and, more important, to their obligation for risk and value-based executive communication.

Single vs. Multi-Sector Benchmarking

Given the diversity of this multi-sector working group, the SEC's opportunity to support the International Association of Hospital Safety and Security (IAHSS) in a similar Metrics Working Group provided the prospect of identifying a body of measures appropriate to what appeared to be a more homogeneous sector. Hospital security represents a unique, physically demarked environment from which to view a security mission thoroughly focused on risk identification and mitigation:

- Typically at the top tier of workplace violence statistics
- Risky patients: psychiatric, babies, dementia, felons under guard
- Risky environments: parking lots, regulated information and controlled substances, perpetrators and victims mixed in ER waiting, higher crime urban locations
- Intense financial pressure on service costs

This metrics initiative was interesting because the sector has an active professional association of over 1,800 members, several of whom saw the need for a body of performance metrics. The group was benchmarked and we repeated the process used previously of engaging a select group of members in discussion on what specific type and content of metrics would have the greatest benefits. A survey with 20 metric examples was sent to the IAHSS membership. Since the audience was new to the discussion, I also included a brief description of the potential use and value for each selection to give the respondent information to aid in their evaluation and ranking. Respondents were asked to rank their selections using the five choices around utility and actionable preference seen in the following chart (Figure 4). The results were tabulated for the top, middle and bottom thirds as shown below.

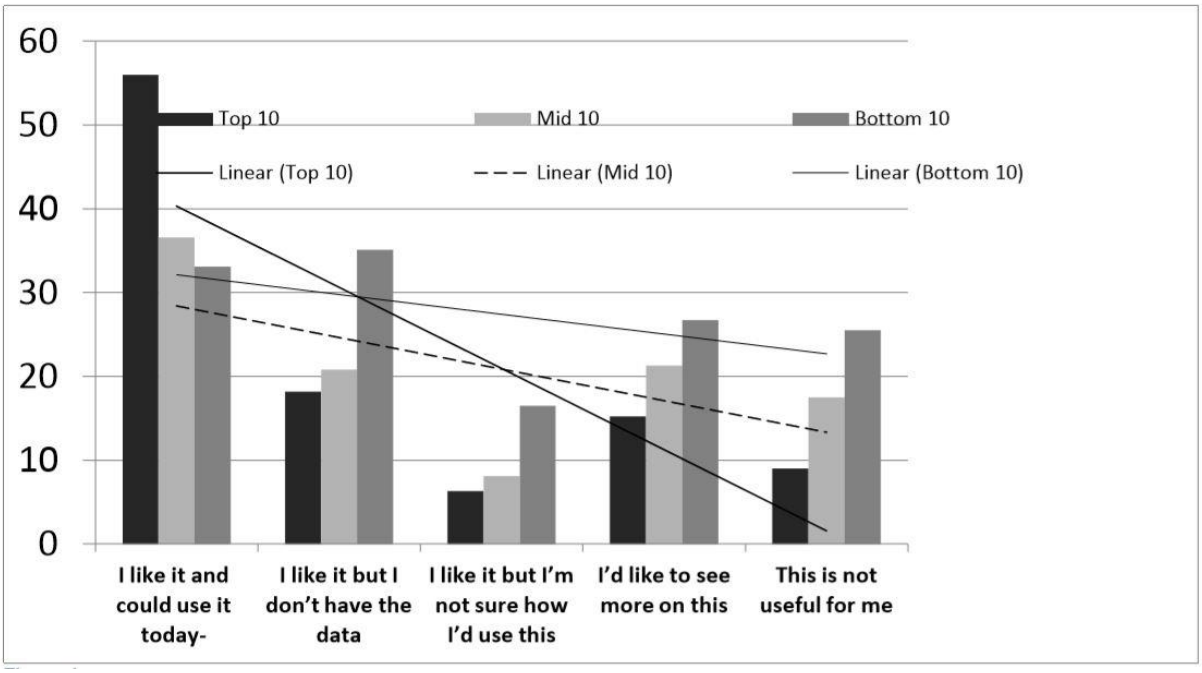

Figure 4

It was hoped that the commonality of health care security services would bring a more level playing field to the results, but the IAHSS displayed some significant differences in service population demographics (urban/rural, public/private, specialty care versus general population, research, etc.) that tended to drive the risk management mission somewhat significantly. The driving assumption on the audience being polled is that they understand the security issues confronting their respective organizations, but their respective institutions' services and service populations vary, often significantly as it bears upon the security mission. This variance consistently has influenced how members viewed the value of specific measures and metrics. The wording in these choice categories was selected to allow for these variances.

Given a choice among a diverse selection of three-dozen metrics, it is not surprising that this organization's members prioritized their top 10 as follows:

1- Aggressive incidents resulting in need for physical intervention or restraints by security

2- Security incident and event demographics

3- Security service (or other specific type) calls per daily guard hour

4- Percent of security incidents resulting from patient mental health/aggressive behavior

5- Aggressive incidents per daily guard hour

6- Workplace violence incidents per 1000 employees

7- Reporter theft per 1000 inpatient days

8- IAHSS or other standards, guidelines or peer-established performance criteria adopted and accepted as compliant

9- Ratio of security officers (first responders) to employees served

10- Security exercises and drills indicate acceptable levels of knowledge of response procedures consistent with potential risk exposure

Given this more common risk landscape, it was interesting that the bottom third of useful metrics were primarily related to a more aggressive approach to risk avoidance and customer satisfaction. Selections here included: 1) security/safety hazards discovered per hour of proactive inspection or patrol, 2) ratio of employees involved as subjects of investigations per 100 employees, and 3) percent of sampled customer interactions rated positive to highly positive. One might have anticipated a desire to be able to advertise these results rather than those seen in the table above. But, while reflecting a response to their risky work settings, this list also demonstrates an undercurrent of pressure on cost containment and the ongoing need to inform and gain support from management. With this group and others we've evaluated, you also get a sense of frustration—a need to remind their customers that security is only a part of the solution and residents need to own a role in protection.

Benchmarking Metrics within a Single Security Program

There are some functions within corporate security organizations that appear to be similar enough in mission and task content to enable reasonable points of comparison. We have explored two such programs in some depth: guard force operations and global security operations centers (GSOC).[7]

Guard force operations typically represent the single biggest expense in most corporate security budgets, so the examination was thought to be a priority for a deeper dive. An extensive database of measures and metrics associated with contract security officer tasks (105 at current count) in multiple categories of service delivery has been documented and tied to candidate contractual and service level agreement (SLA) standards. An extensive list of tasks and performance measures were identified and divided between those that should be incorporated in vendor operations and others that are appropriate to security department measurement of vendor performance.

The GSOC metrics inquiry is the product of a Best Practices working group of about 50 major companies with global security operations centers. Developing metrics is a key element in the proof of best practices. Metrics also provide clear indicators of risk

[7] Background Investigations are another area that would lend itself of metrics comparability. The processes are essentially similar across industry sectors and the risk factors that comprise the areas of examination are well established. These services are largely provided by a number of vendors under contract to Human Resource departments.

mitigation and business alignment value for these core security operations. Metrics in this sample tend to relate to performance measures of staffing and dispatch operations but may also provide more qualitative measures of response to various types of events. Since GSOC is a highly process-centered operation, it is interesting that metrics in this group of practitioners are not more mature and attuned to the measures employed by corporate call centers or public safety dispatch operations.

An interesting view of IT security metrics. This report has noted the relative maturity and expansiveness of the IT sector's inventory of metrics. In 2013[8], the Ponemon Institute surveyed IT professionals in the US and UK regarding the use and effectiveness of their metrics in communicating risk to management. More than half of those surveyed felt their metrics were not effective and "the information is too technical to be understood by non-technical management." Respondents complained that their executives were "not interested" and they "didn't have the time or resources to report to senior executives." The conclusion of this benchmarking was that the "majority are not sure how to distill their data into metrics that are understandable, relevant and actionable to senior business leadership." Here is a group with a well-established, standards-based inventory of measures in an area of enterprise risk acknowledged in most 10-K reports, and their challenges align in many ways with their generalist security colleagues surveyed earlier by the SEC.

Other Benchmarking Efforts

Security 500. For several years, Security magazine has conducted a "Security 500" annual review of corporate security resource data and their representatives' perceptions of issues and concerns relevant to risk trends and security management. Although the published article ranks 500 organizations, the magazine obtains security budget data for less than half that number. This yearly review yields data on security budgets and metrics on spend to employee and revenue as well as other data for some selected industries. Given the difficulty of gathering and affirming even this basic information, this annual initiative deserves real credit for pushing the opportunity to document a few nuggets of comparative data.

The Security Leadership Research Institute (SLRI). The SEC launched the SLRI in 2009 as a direct response to the issue of fairly comparing security elements across peers. Its first Corporate Security Organizational Structure, Cost of Services and Staffing Benchmark consisted of 183 participants. The second iteration of this benchmark is underway at the time of this writing. The SLRI benchmark incorporates input from industry leaders with the goal of providing those leaders a superior tool to use to benchmark against similar organizations. The SEC actively encourages its constituency to involve their industry or sector trade groups. But the latter has proven to be a tough row to hoe. The collapse of

[8] https://www.tripwire.com/state-of-security/risk-based-security-for-executives/risk-management/majority-of-it-professionals-dont-communicate-security-risks/

these potential focus groups has been due to lack of interest and, as stated earlier in this report, a hesitation to share information.

Summary on Benchmarking

These benchmarking activities serve to provide an overview of current practices that have been consistently affirmed in ongoing SEC outreach and client engagement programs for the past seven years. Benchmarking can complement a qualitative metrics program, but the essential measures and building blocks must be tailored to the unique requirements of each budgeted activity in the corporate security organization.

Moving from Benchmarking to In-Depth Capacity-Building Efforts

The SEC continues to work with a number of progressive security executives who see the need to embed a disciplined approach to program measurement across their portfolio of services. In one example the CSO of an outstanding corporate security organization that serves a very successful global manufacturing company launched a major initiative to identify a body of metrics across the security organization "to tell the value story to management to demonstrate in measurable ways where and how we bring value to the bottom line of our company." This highly focused effort involved SEC collaboration with client teams in guard force operations, contingency planning, background vetting, threat and risk assessments, supply chain protection, workplace violence response and a variety of previously un-probed corners of security service delivery. The result of the engagement provided the security organization with a process that leveraged available data from counting to analysis and maintenance of a few key performance and risk indicators that support the value proposition sought by the CSO.

In other examples, various CSOs have identified more focused needs for building or advancing their metrics programs:

- Leverage the data in the incident reporting system to build a multi-year set of key risk indicators focused on the insider risk and the performance of their respective regional security teams
- Identify what data was most appropriate to supporting a specific set of metrics in several categories of program performance
- Identify an approach to building a performance management scheme to include linkage between performance standards and performance measurements and metrics
- Examine data on hand to determine reliable approaches to supporting security's return-on- investment

- Build a body of measures and metrics that link financial results with program performance and risk mitigation
- Focused sector benchmarking on specific security programs

Types of Security Metrics Currently in Play

Security programs deliver a variety of products that have been developed to serve specific clientele or management objectives. Each of those objectives possesses its own unique indicators of quality and effectiveness. Figure 5 portrays a linked set of metric indicators we have found to be an integral part of the security manager's program measurement system, and there are a host of others that serve the tailored requirements of specific programs. This report cannot estimate the frequency of use of these or other metrics by security organizations, but we can recommend that every security executive evaluate the potential utility of each within his or her organization.

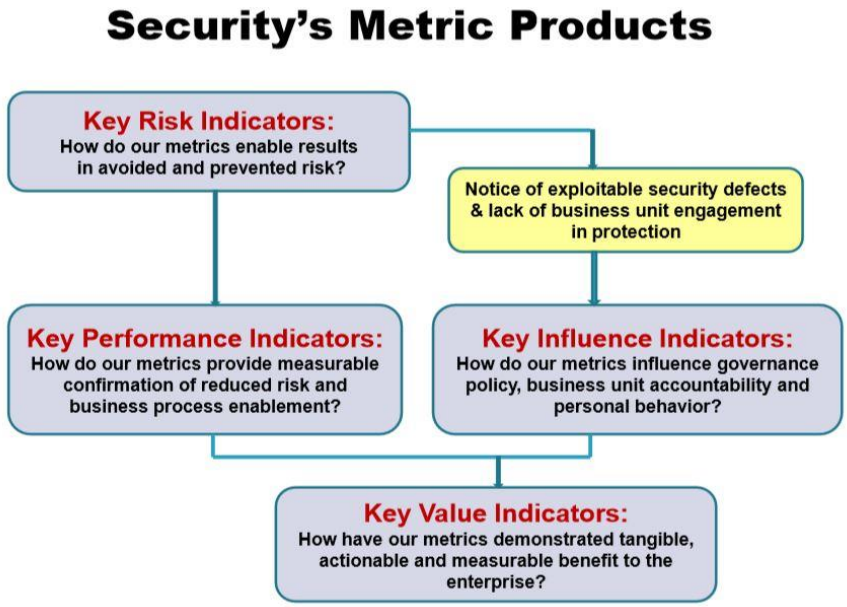

Figure 5

Activity measures and indicators. These are the data gathered in event response that provide the inputs to measurements and analytics. As noted earlier, these are the tallies of incidents, workload, losses, recoveries, places, and a host of other factors that are culled from logs, incident reports and investigations. The process typically results in counts for trending and periodic reporting.

Key performance indicators (KPI) & key risk indicators (KRI). More mature organizations are building a body of KPIs consistent with the quality and performance

measurement systems at work across the enterprise. KPIs are an integral part of business planning and strategy, and KRIs are accepted elements of the enterprise risk management practice. There is a clear linkage between KPIs and KRIs for these organizations: KPIs tell the story about how well risks are being managed by all accountable parties, and KRIs signal the direction a designated risk is headed. They allow these managers to assess the degree to which various control measures enabled risk avoidance and how the results can be leveraged to support resource allocations. Companies employing these indicators are seeking to answer the question, *Is there a defensible line from the elimination of the exploitable security defect to a specifically directed security activity?* These are questions that drive the consideration of a security program's value.

Influence. The security executives in these more mature corporate security organizations leverage their metrics to influence behavior and enterprise policy. They have found that when they have a clear connection between their verifiable metrics and risky business practices, they are more effectively armed to influence accountability in business unit managers and build awareness of responsibility for improved practices and internal controls.

Compliance. In regulated organizations, proof of compliance is an important focus of measurement programs. Incorporating metrics in security processes that contribute to avoidance of non-compliance, provide evidence of best practices for regulators, and measure the results of assurance activities all support compliance management.

Financial and business management. Every security manager is required to have a set of metrics that are tracked for conformance with business objectives and budget burn to plan. Our engagements with practitioners consistently underscore the importance of providing linkage between these data and relevant risk and performance indicators. The result is a more integrated view of security's responsiveness to the dynamics of the business risk environment.

Value. As noted by our benchmark participants, proof of value is almost universally elusive for security executives. It may be relevant that truly effective security is invisible, especially where it is effectively integrated into the daily business. But a consistent complaint from polled security managers is that their business executives typically don't understand what or why security delivers to them. A targeted body of metrics can enable the security manager to craft a story to assist in educating top management on where and how they bring value to business strategy and the bottom line. This message has to include a variety of metrics that demonstrate in business terms the specifics of the value story. Successful security executives are finding that when they do a really solid job of building tangible measures of a program's performance in enabling a positive business result, their metrics become a centerpiece of security's value proposition.

Quality and excellence. Companies with formal quality management programs like Six Sigma, Lean and Operational Excellence actively seek to measure process for quality indicators. While many qualitative metrics are found in the positive results seen in performance measures, many others may go directly to demonstrating a true qualitative measure. Here are a few examples:

- Security Tours: X% improvement in number of hazards identified and mitigated per 24-hour period
- Process Efficiency: Reduction in cycle time by X% or removal of a security process resulting in a Y% reduction in the cost of the process.
- Number of security processes identified from benchmarking as best-in-class.
- Number of customer captures assignable to security practices.
- Modified security procedures deliver X% increase in worker safety and Y% reduction in workplace injuries.

Metrics as a centerpiece of a corporate security communication strategy. Security executives in these various surveys and group initiatives universally cited the need to deliver a more compelling story regarding the program's value and contribution to global business strategy and objectives. There is a small but growing group of senior practitioners who clearly see their metrics as a centerpiece of a more formalized communication strategy. They see the opportunity to "market" the performance of various risk mitigation programs and use the lessons learned to influence the highest echelons of executive management. This level of visibility in greater numbers of practitioners will significantly contribute to expanding the scope and impact of corporate security metrics programs.

Metrics Maturity Measurement

The SEC's extensive collaboration with corporate security programs over the past decade has enabled us to document a set of evaluative criteria for a security metrics program. We have identified twelve factors that comprise the basic elements of a formal program and three performance levels that tend to mark program maturity. These are provided as a table in Appendix 1.

Challenges and Opportunities

Challenge - The clear relevance and acceptance of performance measurement in business management is not adequately reflected in established security management practices.

Measuring business process effectiveness and how well resourced activities are contributing to the success of the business is a basic expectation of management. But when we look objectively at the state of the art of corporate security's measurements and metrics, the picture that emerges is clear: While there are pockets of solid examples, there is no established framework and there are no consensus standards or best practices for corporate or enterprise-wide performance measurements. There are visible incentives all across the risk and management landscape, but these have not coalesced to prompt cross- or even inter-disciplinary consideration. This gap in our performance management knowledge base deserves action from industry leaders.

Challenge - A fundamental metric that should be in every security executive's portfolio is a maintained documentation on the total cost of security to the enterprise.

It's a commonsense question from a CEO or CFO and yet, how many security executives could answer it with some level of accuracy? What are the operating and variable costs? What is the cost of regulation to the enterprise? If the mandate is to reduce cost, why simply look to the direct security budget for the total contribution? Security task costs touch every business activity in some form or another and impact productivity and profitability. This is a metric worth the hunt.

Challenge - Enterprise-wide security issues lack appropriate visibility in the formal enterprise risk management agenda.

Sarbanes-Oxley and several other legislative initiatives in the past several years have given significantly increased executive and board visibility to enterprise risk management (ERM). Unfortunately, a search of the literature fails to find the range of operational and reputational risks within the scope of corporate security operations. Metrics in these areas of event response and investigation are essential to effectively connect the dots on root causes and more integrated approaches to mitigation. CSOs directing the more mature and well-established security programs have pushed their program's metrics and documented results on to senior management's ERM agendas, but far too many programs are failing to influence these critical and more inclusive views of enterprise risk.

Challenge - There is a need for an established framework for enterprise security performance measurement.

Under the auspices of a variety of industry sources, IT has established and affirmed a standards-based framework for, if not mandatory, at least essential security controls. A measure of acceptance of these best practices is their incorporation as audit standards. The largely remaining elements of enterprise security have individually and collectively failed to evaluate and build a similar framework to drive performance standards, measurements and metrics. In spite of the barriers, it would be beneficial to develop a baseline of security metrics that apply in each security discipline, in and across each sector. This would allow the security community to engage in meaningful discussion and

consensus on performance standards that would measurably contribute to broader professional standards. In order for this type of disciplined high-level discussion to take place in security, some entity or a partnership of entities must first take the initiative to accept that real performance and risk measurement in corporate security is critical to a more accepted and fundamental role in enterprise risk management. So far, and aside from our limited SEC initiatives noted here, no such non-IT entity has emerged in either the public or the private sector. This is an initiative worth wider discussion among established industry groups.

Challenge & Opportunity - Develop a few key (transferable) performance and risk-related metrics for each security discipline.

Why not have 3-5 performance metrics for each functional element in a full-service enterprise security operation? Why not specify a high-level set of security-related risks that confront global corporations and link to 3-5 key risk indicators that companies could adopt for evaluation, modification and possible incorporation in their metrics program? What shared experience might we explore if there were a body of performance metrics that were linked to those commonly shared areas of risk? Might this drive practitioner discussion around transferable best practices in performance-based countermeasures, technology application and other approaches to enterprise protection?

Here are a few examples of possible collaborations between security disciplines and related professional associations that could engage their members in the consideration and development of performance measures.

Discipline	**Partners in performance measurement collaboration**
1- Background investigations (BI)	Society of Human Resource Management
2- Investigations	Risk & Insurance Management Society (RIMS), Institute of Internal Auditors, Association of Certified Fraud Examiners, American Bar Association
3- Uniformed Security Operations	National Association of Security Companies, ASIS International
4- Security Technology	Security Industry Association, Central Station Alarm Association, National Fire Prevention Association
5- Supply Chain Security	Council of Supply Chain Management Professionals
6- General Security Management	Security Executive Council, ASIS International, Business Roundtable
7- Information Security	SANS Institute, Carnegie Mellon, Information

	Systems Audit & Control Association
8- Research	Mitre Corporation, Sandia National Laboratory, National Institute for Standards & Technology (NIST)
9- Financial Implications of Security Programs	University-level business schools

The value story is compelling when it speaks the language of finance, and it's likely true that mathematical proof of return plays more convincingly than building a case that demonstrates a security measure's effectiveness in preventing a crime. A simple equation for determining return on security investment (ROSI)[9] is as follows:

$$\text{RoSI} = \frac{\text{Risk Exposure \% Risk Mitigated} - \text{Solution Cost}}{\text{Solution Cost}}$$

The attractiveness of RoSI to many security executives and practitioners is heightened in the competition for limited resources. Management seeks to maximize the benefit of its investments, and the security literature is replete with a variety of models purporting to reveal an approach with demonstrated effectiveness—most in the IT security space where the benefits can be more readily machine-measured. The RoSI of well-executed background investigations and risk assessments that uncover exploitable vulnerabilities are obvious to experienced security executives but are challenged by the clarity of a revenue-enhancing business process with an RoI of 200% in twelve months.

A collaborative effort between business school academics, finance, and corporate security executives to develop a body of models keyed to various security disciplines could contribute greatly to enabling CSOs' documentation of RoSI for top management.

Opportunity - There is an increased senior management and board acceptance of security's contribution to the enterprise risk management agenda.

As can be seen in Appendix 2, when the SEC's first book on Metrics was published in 2007 there was relatively little in the way of industry-wide discussion, let alone established literature on corporate security metrics. Since then, management has increasingly pushed the alignment and cost-efficiency of non-revenue producing departments. CSOs are increasingly in front of senior management and Boards of Directors or their risk committee. This access will support the need for maintaining a select few metrics that can summarize, inform and influence on key issues. Corporate security's scope of risk visibility and engagement is more global, and the more mature,

[9] Journal of Research and Practice in Information Technology, Vol. 38, No. 1, February 2006, page 56

well-established programs are far more present at the enterprise risk management table. Supply chain resilience, cyber threats and concern for business continuity are likely to be included in every corporate 10-K form.

Opportunity - The recognition of metrics' value by security managers is increasing.

This applies to a more selected and informed group of senior security executives but generally as confirmed in our earlier benchmarking, security executives are more engaged in identifying a few key metrics appropriate to their risk and business environments and using those in justifying cost and demonstrating the specifics of contribution to the bottom line. Further support is found in the 2013 Ponemon Institute study noted earlier, which stated that when security managers were asked how important they felt metrics were in achieving a mature, risk-based security management process, 75 percent indicated "very important" or "important."[10]We have also noted our experience with some security executives who are doing far deeper dives into metrics development, dashboard construction and executive communication. Many executives have found that telling the value story has taken on a higher profile as the internal competition for resources becomes more intense.

Opportunity - Growth in regulations presents a need for compliance measurement and management.

The SEC has documented the expansive scope of applicable security-related regulations and standards in its Regulations and Compliance Management database. The implications of non-compliance to brand reputation clearly point to a need for security managers to develop responsive safeguards with accompanying performance measures, proactively monitor compliance, and inform management on gaps in compliance.

Because standards typically require demonstration of measured conformance is an additional incentive. Take NFPA 1600[11] as an example: "The entity shall identify hazards, the likelihood of their occurrence, and the vulnerability of people, property, the environment, and the entity itself to those hazards." The explanatory material interprets this section in part by noting that the analysis "should give a clear idea of what hazards are most likely to occur; what entity, facilities, functions, or services are affected based on their vulnerability to that hazard; what actions will most effectively protect them; and the potential impact on the entity in quantifiable terms." "Quantifiable" means just what it says- it is demonstrated in measured, metric terms.

Opportunity - Industry groups and security-related professional, trade and vendor associations have a clear stake in developing, owning and sharing measures and metrics appropriate to their represented security disciplines and business practices.

[10] The State of Risk-Based Security Management, Ponemon Institute, 2013, page 2
[11] NFPA 1600, Standard on Disaster/Emergency Management and Business Continuity Programs, 2013 Edition, National Fire Protection Association, Quincy, MA

Prior to and more intensively after 9/11, industry groups have been engaged in security-related initiatives related to critical infrastructure protection and programs for information sharing. An example of industry leadership is the American Chemistry Council's involvement with DHS in the Chemical Facility Anti-Terrorism Standards Regulation (CFATS). CFATS is particularly interesting in the metrics space due to the incorporation of a risk-based performance measurement system with applicable metrics for each safeguard subsystem.

Security associations, organizations and sector publications have all stepped into security measures benchmarking and development. On the vendor side, we have seen some industry-specific collaborations emerging from regulatory initiatives (healthcare, chemical and electric are examples). This could contribute to developing best practices, support the identification of outliers and establish a common set of performance standards to be incorporated in Service Level Agreements- all positives for clients and service providers alike.

Shared metrics within specific disciplines can measurably raise the bar for the industry. For example, background investigation processes are similar with a relatively mature selection of performance measures. The SEC's examination of multiple company practices for guard force operations and security operations centers found an expansive inventory of measures and metrics that may be applied across the diversity of sector, risk and operational environments being served.

The SEC has invested significant time and effort into developing and communicating a number of cross-sector risk and performance measures and metrics. But no other professional industry group has yet announced an effort toward developing security metrics that can be considered for use across within their sector or across various sectors in the security industry. The SEC is eager to participate and share our experience, but it's likely that such an effort could only succeed if industry groups worked together and encouraged all their members and constituencies to participate in a joint effort.

Opportunity - Identify best practices in self-directed metrics development.

The SEC has experience with several organizations that have identified a variety of unique metrics keyed to their specific business risk requirements. This is an example of a distributed body of knowledge that could be shared if there were an established platform for wider distribution, vetting and application.

Opportunity - Exploring Operational Excellence (OpEx) in security program management.

The SEC is supporting several progressive security executives' focus upon the application of operational excellence disciplines within their program management objectives.

Measurement of program results is a key element in OpEx, and these efforts hold promise for advertising a framework for key performance metrics.

Opportunity - Improved incident reporting, case management and analytical applications facilitate metrics development and management.

A highly positive trend that contributes directly to the development and delivery of quality security metrics is the maturity and expanding use of reporting and data management applications like PPM2000 and others. They provide a disciplined set of processes around incident reporting and analysis that are absolutely essential to a qualitative metrics program. Disciplined data management can enable corporate security in collaborating with the governance team and in focusing its data on connecting the dots to yield a consolidated vs. siloed picture of risk. The result can be extremely informative and actionable. Incident reports, investigations, risk assessments, tests and other sources of risk-related data are replete with leading and lagging indicators that can feed more intelligent learning systems. A number of companies are pushing the envelope in predictive analytics with a variety of applications in statistical analysis, modeling, situational analysis and data mining to predict and alert to future risk.

Opportunity - Learn from IT security colleagues.

Information Security Officers have developed a rich foundation of metrics and an extensive body of literature to formalize acceptance across this sector. It may be that the discipline behind them has a variety of transferable opportunities to be explored. Inter-disciplinary collaboration could jump start a set of coordinated key risk and key performance indicators as well as the process driving their utility for a wider group of security managers. This report acknowledges the deep inventory of metrics the IT sector has collaboratively developed, and there are undoubtedly other risk or performance-centered examples flying below the radar.

In the spirit of the challenges and the need for consideration of opportunities, the following from Andrew Jaquith is worth a closing comment:

> "For any game, without a way to score the play, you cannot improve your performance as a player. That is where we are today; no way to score the game and no way to improve our play. This is not just a failing; it is a risk in and of itself. If we cannot make headway on measuring, on scoring, on understanding our risks well enough to change the odds in our favor by backstopping decisions about risk, we will have created one of those vacuums that Nature abhors. If we cannot find a way to measure the security problem, I am afraid our choices will become difficult."[12]

[12] Security Metrics- Replacing Fear, Uncertainty, and Doubt, Andrew Jaquith, Addison-Wesley, 2007, pg. xvii

A Closing Note on Current Practices

This paper is built on the premise that measurably effective management of enterprise security requires a body of performance measures and metrics and, while there are a variety of available sources, no accepted collection exists to drive standards and best practices. We have suggested a number of approaches to building consensus around such a collection and processes for their review and acceptance.

The findings and opinions expressed in this assessment are based on the significant time and effort the Security Executive Council has invested in a variety of engagements with practitioners and in building, testing and fielding an inventory of corporate security metrics across multiple industry platforms and exchanges. Our perspective is admittedly limited to those relationships and initiatives to which we have been privileged to contribute. There are untallied numbers of ideas and examples from experienced professionals within and outside our craft that need to be mined for opportunities to expand our learning and delivering richer evidence of security's value.

We hope that this paper will contribute to bringing those professionals and their ideas to the table.

Appendices

Appendix 1: Measuring the Scope and Quality of the Security Metrics Program

Over the past decade, the SEC's continuing relationships with scores of corporate security programs have provided the opportunity to identify the various factors that contribute to reliable, actionable and effective metrics. While there are other factors we might employ, the twelve in the following table serve well to summarize a level of maturity and resulting benefit to both the security organization and the business it serves.

Corporate Security Metrics Program Maturity			
Factor	**Lower Maturity & Acceptance**		**High Maturity & Benefit**
1. Organizational Context for Security Metrics	*1.1 Metrics are an accepted element within selected business operations but have not been requested by Security*	*1.2 Management is beginning to seek performance measures & metrics from Security*	*1.3 Performance measures & metrics are a required element of program management*
2. Current Status of Metrics within the Security Department	*2.1 Recognized need and established objective but in very early stages of development*	*2.2 We have several focused metrics outputs for targeted constituents but now want to elevate the content for management or the Board*	*2.3 We have a well established program with quality reporting and now desire to develop a more directed and influential set of measures and metrics*
3. Availability of Data for Metrics Development	*3.1 We do not currently have a centralized incident reporting system*	*3.2 We have a limited incident reporting database that is distributed among multiple security-related functions*	*3.3 We have an enterprise-wide incident reporting and case management system that enables reporting of desired metrics*
4. The Level of Reliability of the Available Data	*4.1 Our incident and performance-related data does not currently have consistent standards of review and reliability*	*4.2 Although our incident and performance-related data is distributed among multiple organizational units, there are consistent standards of review and reliability for*	*4.3 We have an enterprise-wide incident and performance-related data repository with consistent standards of review and reliability*

		reporting up	
5. Analytical Scope & Discipline	*5.1 Current processing of incident and performance data is primarily limited to maintaining counts of various data elements for trend analysis and reporting*	*5.2 A limited number of security programs are thoroughly analyzed for qualitative and quantitative findings and targeted reporting*	*5.3 All security programs are subjected to ongoing qualitative and quantitative measurement with metrics outputs available for management reporting*
6. Analytical Benefits of a Security Metrics Program	*6.1 While it is an objective, we do not currently provide a measurable level of analysis to our incident and program performance data*	*6.2 We see measurable results when we provide analyses of business unit risk exposure and security advice to business units*	*6.3 Our analysis of security program performance has enabled demonstrably improved management understanding of the value of security investments*
7. Reporting	*7.1 Reporting is primarily for internal security department program performance tracking*	*7.2 Formal reporting of program performance data is limited to a select few key indicators required by management*	*7.3 We provide a variety of standardized and tailored metrics reports to management on an established schedule*
8. Directional Performance Standards & Guidelines	*8.1 We currently do not employ an established body of industry or locally developed performance standards or guidelines that may be used as benchmark targets for metrics*	*8.2 We have adopted a selected set of measurable performance standards or guidelines developed by others that are tracked and reported to management*	*8.3 We have both adopted externally produced performance standards and developed others appropriate to our unique business management requirements*
9. Actionability	*9.1 Our metrics are limited to occasional reports that are primarily designed to inform on status of selected trends over time*	*9.2 We are in the process of developing a body of metrics that may be used to measure the value and effectiveness of security programs*	*9.3 Our metrics are primarily analyzed and delivered to affirm positive business unit action or advise and direct corrective actions*
10. Resources & Tools	*10.1 Resource constraints currently limit our ability to maintain an effective security metrics program*	*10.2 Each security manager is required to maintain basic performance metrics for each of their assigned programs*	*10.3 We devote adequate staff time and employ a robust set of applications to maintain and deliver a variety of metrics reports to management*
11. Data Sensitivity &	*11.1 Our incident and*	*11.2 There are safeguards that protect the*	

Protection	*trend data is not considered sensitive enough to warrant special protection*	*confidentiality of metrics data that could reveal potentially risky information to unauthorized individuals or present litigation risk.*	
12. Summary Assessment-Measuring Security's Value to the Enterprise	*12.1 We are actively seeking a body of metrics capable of demonstrating measurable value to the enterprise*	*12.2 We have a few metrics that have been requested by individual departments*	*12.3 We have a robust body of metrics accepted by management as demonstrating measurable value to the enterprise*

Summary

The notion of maturity level in security metrics management is directly relevant to what SEC research has revealed in terms of security executives' approaches to measuring their programs and then directing risk and performance metrics to management. The more progressive CSOs have identified key risk and performance measures and push the results to inform, influence business strategy and communicate security's value proposition.

Appendix 2: References and Sources of Information on Security Metrics

The following represents a reasonably broad sample of publications on the subject of security measurements and metrics. Sources devoted specifically to information security have an asterisk (*).

*Brotby, W.K. (2009). Information Security Management Metrics, A Definitive Guide to Effective Security Monitoring & Measurement. Auerbach Publications.

*Brotby, W.K., & Hinson, G. (2013). Pragmatic Security Metrics: Applying Metametrics to Information Security. Auerbach Publications.

Campbell, G. (2011). Driving Excellence in Enterprise Security. Security Executive Council. Retrieved from: https://www.securityexecutivecouncil.com/spotlight/?sid=27289

Campbell, G. (2007). Measures & Metrics in Corporate Security: Communicating Business Value. Security Executive Council.

Campbell, G. (2009-14). Monthly column: Metrics for Success. Security Technology Executive Magazine. Retrieved from: http://www.securityinfowatch.com/magazine/

Gollmann, D., Massacci, F., & Yautsiukhin, A. (2006). Trade Paper Quality of Protection: Security Measurements and Metrics. Springer.

*Hayden, L. (2010). IT Security Metrics A Practical Framework for Measuring Security & Protecting Data. McGraw Hill.

Hayes, B., & Kotwica, K. (September 2011). Benchmarks Aren't Magic, They're Tools. Security Magazine. Retrieved from http://www.securitymagazine.com/articles/82320-benchmarks-arent-magic-theyre-tools

*Herrmann, D. (2007). Complete Guide to Security and Privacy Metrics. Auerbach Publications.

Hubbard, D. (2010). How To Measure Anything: Finding the Value of "Intangibles" in Business, 2nd Ed. John Wiley & Son, Inc.

Interagency Security Committee (2009). Use of Physical Security Performance Measures. (2009). Retrieved from http://www.dhs.gov/xlibrary/assets/isc_physical_security_performance_measures.pdf

*ISO 27000 Directory. (2009). Introduction to ISO 27004: Information Security System Management Measurement and Metrics. Retrieved from: http://www.27000.org/iso-27004.htm

Jansen, W. (2009). Directions in Security Metrics Research. NISTIR 7564. National Institute of Standards and Technology.

*Jaquith, A. (2007). Security Metrics: Replacing Fear, Uncertainty, and Doubt. Addison-Wesley.

Kotwica, K., & Blades, M. (2008). Marking the Yardstick. Access Control Magazine. Retrieved from: http://securitysolutions.com/enduser/enterprisecorporate/marking_yardstick_security_program/

Kovacich, G., & Halibozek, E. (2006). Security Metrics Management, How to Manage the Costs of an Assets Protection Program. Elsevier Butterworth-Heinemann.

*Payne, S. (2006). A Guide to Security Metrics, SANS Institute Security Essentials. Retrieved from http://www.sans.org/information-security

*Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. (2005). Corporate Information Security Working Group: Report of the Best Practices and Metrics Teams. Government Reform Committee, U.S. House of Representatives.

*Wong, C. (2011). Security Metrics, A Beginners Guide. McGraw-Hill.

The following are publications that can assist the reader in designing metrics presentations and presenting analytical information:

Abela, A. (2008). Advanced Presentations by Design: Creating Communication That Drives Action. Pfeiffer.

Abela, A. (2010) The Presentation- A Story About Communicating With Very Few Slides. CreateSpace Independent Publishing Platform.

Few, S. (2006). Information Dashboard Design: the Effective Communication of Data. O'Reilly Media. Few, S. (2004). Show Me the Numbers, Designing Tables and Graphs to Enlighten. Analytics Press.
Few, S. (2009). Now You See It: Simple Visualization Techniques for Quantitative Analysis. Analytics Press. Person, R. (2009). Balanced Scorecards and Operational Dashboards With Microsoft Excel. Wiley.

Tufte, E.R. (2006). The Cognitive Style of PowerPoint: Pitching Out Corrupts Within. Graphics Press LLC.

Visit the Security Executive Council website for other resources in the Demonstrating Value: Measuring Value 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 here: https://www.securityexecutivecouncil.com/