EXCERPT

ELSEVIER'S SECURITY EXECUTIVE COUNCIL
RISK MANAGEMENT PORTFOLIO

MEASURING AND COMMUNICATING SECURITY'S VALUE

A COMPENDIUM OF METRICS FOR ENTERPRISE PROTECTION

GEORGE K. CAMPBELL

Security Executive Council

CONTENTS

Excerpt from the book's Forward by David Komendat, Chief Security Officer, Boeing Corporation
"Boeing's initial journey to develop a body of security metrics was not easy. We first had to educate the middle management of our organization on the value of creating metrics. George Campbell, the author of this book was our guide in this journey. I'll never forget George's initial assessment of our security and fire protection organization. "You have great people, a ton of data and world class services," he stated. "But, you don't do anything of value with the data. Your security and fire leaders don't understand how to create metrics and you aren't telling your story effectively at all." It was a sobering moment.

So began our metrics journey in late 2010. Fast forwarding to today, we have developed an impressive suite of metrics that capture nearly every service offering within our security and fire protection organization. These metrics allow me to quickly and effectively communicate the value, quality, cycle time and cost avoidance created by the investment made by the company to protect our people, property, information and providing business resiliency. Each of my security and fire leaders are now able to tell "the bigger story" via our metric package with our internal business partners. Leaders can now easily brief the effectiveness of security and fire protection, even if they don't manage them, because we have spent the time learning about each others' functions and how we collectively bring value to our company.

Three years ago, I had my first opportunity to walk through sections of my metric suite with our CEO and other senior leaders within our corporation. The briefing created an invaluable dialogue for our organization. It was clear that our value story resonated with our CEO and his leadership team. I truly believe the perception and expectations of our security and fire protection organization changed that day in a very positive way.

George's work within the field of security metrics is unparalleled. As you walk through his stories and examples, you will discover that each are based on years of practical learning and experience as a CSO. The knowledge you will gain will undoubtedly help you "tell your story" in the most effective way possible!"

Some Notes to the Reader on Using This Book
If there is one thematic target that should guide the metrics hunt, it is that of value - how should it be defined, measured and presented it in a portfolio of security metrics? It is likely doubtful that Security's value has a uniform definition for every company that has an established security department. However, it may be said that an ability to effectively communicate and advertise how enterprise protection solutions contribute value to the business is related to an ability to inform and tell stories around solid, well-crafted security metrics.

The following stories have been organized to build on a principal theme of having metrics that demonstrate the security department's value to the corporation. The objective with these examples is simply to plant seeds and prompt ideas. If there were an ideal scenario for this work, it would be around the discovery of how to put that data of yours to work in ways you have not yet tried and with positive results you had not envisioned or thought possible.

Here are brief summaries on the half dozen categories. I hope they contain a few gems that will work in your security organization.

Beginnings The initial collection focuses on the why, what and how of a security metrics program. Since so much of what is being learned about this subject on my own and from reviewing scores of others' programs has illustrated the lack of attention to the basics, I thought these few pages would help the reader get grounded on some key concepts I think are essential measures of a metrics program.

Risk I'm also strongly biased toward focusing our measures and metrics on risk; after all, *it's why we have a job*. We add value where we enable the business to avoid risk and an element of that enablement is actionable information and a centerpiece should be our metrics reporting. Thus, a brief cross-section of examples to consider and hopefully prompt ideas for your own risk reporting. I also link this perspective on risk to a section on our ability to influence corporate policy and behavior.

Insider Risk This is what should keep every CEO awake at night and we have a unique perch from which to view risk exposure and influence accountability…or at least eliminate plausible denial. Depending on the reader's security program involvement, understanding our opportunities to provide a lens on reputational risk and corporate integrity is a valuable metrics product offering.

Influence I see our ability to influence as a key performance indicator. Our metrics are the products of our marketing and communications strategy. When they are accurate, timely, informative and actionable they can tell a story that no other member of the enterprise risk management and corporate governance team can bring to the table. I believe every security manager should consider having a few key influence indicators focused on the actionable needs of their primary customers.

How well connected are we to the business? How should we measure our partnership with core business strategy and process? If you can see how our ability to influence through metrics could serve a customer in avoiding a risk, what other information could provide a valued perspective to a business decision-maker? A faster, more secure supply chain? Improved cycle times for hiring and access? A safer workplace or elimination of hazards that cause critical process interruption? Good opportunities for metrics are here as well.

How well are Security's varied programs performing and why does it make a difference? Key performance measures are an integral element of business management. Every Security program has embedded objectives that define the desired results require measurement - and measurements deliver metrics. Additionally, cycle time, customer satisfaction, SLAs, regulatory compliance, benchmarking and other means of performance provide qualitative reporting opportunities for security management.

Building your metrics for impact and results Don't waste time building a metric unless you have a clear idea about what result you want it to achieve. The articles in this book all contain a snapshot of one or more results that should be the intent or anticipated result of the metric(s) discussed. Iwould hope this will prompt your consideration of a potential benefit to your program.

Building the knowledge base is a shared exercise In addition to my own experience and probing, much of what you will find in here is the result of a lot of discussions and idea sharing with a lot of really smart colleagues from across global security organizations. As you consider and hopefully apply some of the concepts contained in this book, I hope you will share that experience and your applications with me. What worked and what did not and why? What is missing here that you hoped you would find? You can reach me at contact@secleader.com.

From Chapter 2: Quantifying and Communicating on Enterprise Risk

If we have done our job, our security measures have been designed and vetted to address what we believe are credible threats or hazards. We know the desire is out there (or in here) with the bad guys and what they scope out is the opportunity. Measurably reducing that perceived opportunity is grounded in the notion of prevention and avoidance. If we fail to act on well-established red flags around fraud, workplace violence or industrial

accidents, we contribute to opportunity and the metrics of probability. When we test for gaps in internal controls and defects in security measures and then communicate the what, where and how of these exposures *to the right people*, we are providing the foreknowledge of prevention.

So, can I absolutely prove that that door you keep propping open will result in a security incident? No. But when it does happen, I'm not going to be the one who the lawyers are looking for.

Of course it's avoidable. And therein lies a key measure of the effectiveness of a well-communicated, security metric. Good security programs and internal controls are built with the objective of preventing and thereby avoiding risk. Think about how you view a trend and then assemble the data you have available in a way that reveals an exploitable gap in a security measure. Now you have the opportunity - the obligation - to leverage that data to point out the accountability for mitigation. You have put your work product in motion to enable future risk avoidance. While you consider this, think about how you might make a clear connection between a risk avoided and the return on the security investment that enabled that result.

Does a CSO have *legal* obligation to inform management about risk? Is there a fiduciary obligation? Regardless of the legality and without question, we have an obligation to inform, educate and advise. Our scope and lens on risk is unique within the governance infrastructure. Our programs reveal volumes on business unit attentiveness to enterprise protection - a window to broader issues of risk management. I believe one of the most critical, value-centered and influential management reporting obligations security managers have is to provide relevant (KRI) to their corporate management and, through appropriate gates, to the board.

I have a bias on KPIs. I think in our business they have to be tied to KRIs and tell the story about how well those risks are being managed by all the accountable parties. This notion of accountability is important. We are only a part of the protection equation, and although we may own the tool kit and a big piece of the rule book, enterprise protection lives or dies in attentive business processes. I think it's fair to say that a good KRI signals a clear indication of which direction a designated risk is headed. Have our control measures enabled risk avoidance? What results are we using to obtain that conclusion? Is there a defensible line from the elimination of the exploitable security defect to a specifically directed security activity? Isn't this the focus of our planning and that positive result the key measure of this program's performance?

From Chapter 3: Measuring Security Program Performance

Risk: Key risk indicators for physical security typically will focus on the consequences of vulnerabilities and defects in countermeasures. Physical security components within site security plans should contain performance measures. Proactive risk assessments and reactive, incident-based lessons-learned and root cause analyses all should ensure the development of metrics tied to findings and recommendations.

Cost: The people, vendors, and technology related to physical security operations are likely the single largest set of cost centers in a corporate security budget. Budgetary line items related to these programs must be based on measurable results beyond burn rates and activity counts.

Contract guard services: In a comprehensive benchmarking review of these vendors, we were able to fairly easily identify almost 100 measurable elements of work associated with contractually based security services. SLAs are

too often unnecessarily constrained by procurement templates and coemployment phobia to apply real (not administrative) performance measures to these services.

Time: Time is a key physical security performance measure. On the one hand, we want to impose time on the adversary and from our perspective we want to ensure we will respond as quickly as possible to all matters requiring timely reaction. Barrier delay time, time to traverse a clear zone, time to reach an asset and escape undetected, and a host of similar measures all contribute to or constrain an adversary. When our security resources deter and delay enough or respond better than required, time becomes a qualitative measure of mission accomplishment.

Access management is measurable: Capabilities to limit unauthorized access and enable that which has been preapproved are clearly measurable elements of both physical and logical security administration. There is an incredibly rich array of industry standard measures that should be employed in this area.

Activities and component capabilities linked to command, control, and communications are measurable: The transaction cycle of event management from initiation, notification, reception, situational analysis, evaluation, dispatch, response, and post-event follow-up contain associated measures of reliability and quality.

Technology-based detection and assessment effectiveness is measurable: This should be focused on measuring reliability. I would hope that any deployment of this huge inventory of security technology has been guided by tested measures of detection reliability, assessment performance, time to failure and repair, and my favorite: false and nuisance alarm rates.

Personnel recruitment, training, and competence: Performance measurement of proprietary or contract personnel is a compulsory responsibility of management, and criteria are well established in HR terms or should be in contractual or SLA terms as well. The effectiveness of recruitment programs is measurable as is the relationship of training to performance.

Measuring operational effectiveness and quality of response: Given the critical first responder mission of these resources, this is the core element of security operations management. Hazard and risk mitigation, response in crises, contributions to business process execution, safe and secure workplaces, planned versus achieved results, customer satisfaction, and measurable results around hundreds of tasks and activities that comprise security plans and procedures all contribute to a required evaluation of physical security effectiveness.

You will better appreciate the fact that measurement begins at home when you have that one-on-one with the Chief Executive Officer (CEO) or Chief Financial Officer (CFO) who asks, “How do you measure our programs and their contribution to the bottom line?” I don’t know how you can define and sell a security program without having the means and, ultimately, the evidence that measure how well it’s working. But apparently the security manager who says, “Nobody’s asking and I don’t have the data” has somehow escaped the obvious oversight by management or is simply waiting for the shoe to drop on career advancement.

Let me be blunt. I believe the security manager who fails to collect, validate and communicate risk and performance measures is contributing to risk.

Sample of Charts:

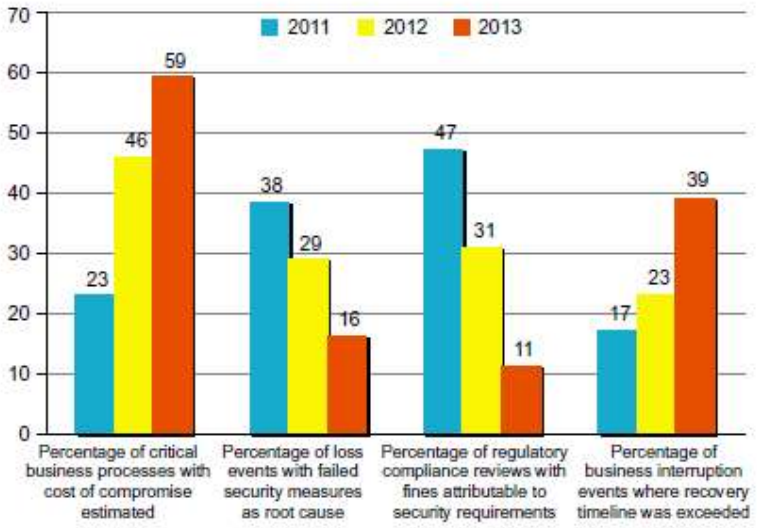
Spreadsheets & Counts Don't Tell The Story

The Data (The "Metrics")

Activity	January	February	March	April	May	June
Initial Background Investigations Processed	14	27	32	21	37	46
Periodic Reviews Processed	3	3	13	10	8	17
SF-86 & Fingerprints Processed	4	2	10	11	6	8
Orientation & Refresher Briefings	7	10	12	6	15	21
Security Policies Developed	2		2	3		1
Data Spill Mitigation/ Incidents	1		1		3	
Secure Area Alarm Responses	3	11	5	22	7	14
Internal Incidents/ Investigations	5	3	2	2	6	1
Foreign Travel Briefings	5		5	3	7	
Visit Requests Processed	2	25	30	8	6	11

The Story

- Cost per case? Cycle time? Rejection rates & causes?
- Cycle time? Retention rates by test? Incident post-mortems?
- Compliance rates? Cost to revenue Centers? Impact on need?
- Severity? Cost per spill? Cycle time to resolution? Where?
- Severity? Cost of resolution? Root Cause? Where? Who?
- # trips to high risk destinations? # trips with/without briefings?



About the Security Executive Council (SEC):

We are a research and advisory firm for security leaders. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year "retained" services agreements (Tier 1 Leaders). Tier 1 Leaders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us seeking a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us at: contact@secleader.com

Learn more: www.securityexecutivecouncil.com