ELSEVIER

ELSEVIER'S SECURITY EXECUTIVE COUNCIL
RISK MANAGEMENT PORTFOLIO

MEASURES AND METRICS IN CORPORATE SECURITY

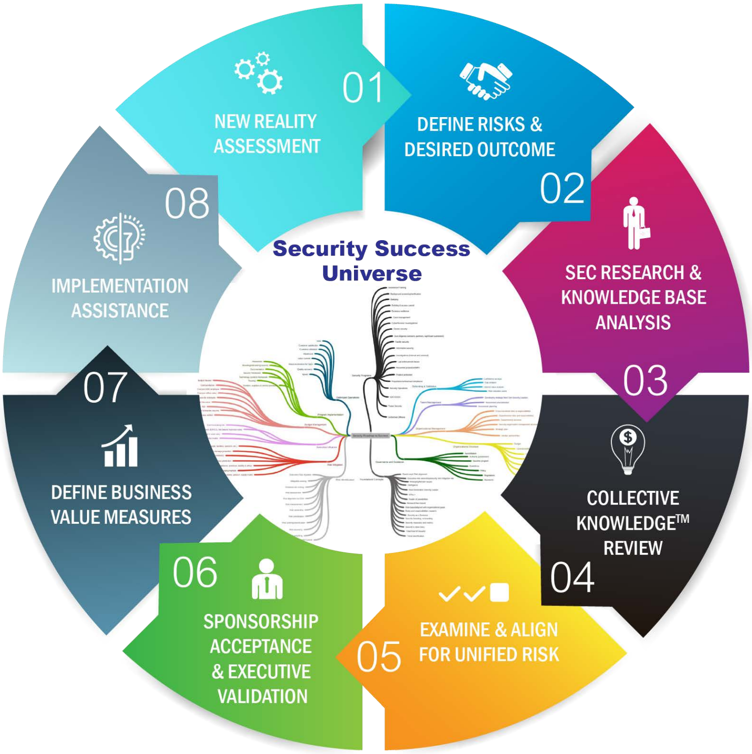
SECOND EDITION

GEORGE K. CAMPBELL

Security
Executive Council

THE SEC PROCESS

We walk clients through eight critical steps to reach their goals


01
NEW REALITY ASSESSMENT
DEFINE RISKS & DESIRED OUTCOME
02
SEC RESEARCH & KNOWLEDGE BASE ANALYSIS
03
COLLECTIVE KNOWLEDGE™ REVIEW
04
EXAMINE & ALIGN FOR UNIFIED RISK
05
06
SPONSORSHIP ACCEPTANCE & EXECUTIVE VALIDATION
07
DEFINE BUSINESS VALUE MEASURES
08
IMPLEMENTATION ASSISTANCE
Security Success Universe

01 NEW REALITY ASSESSMENT

The first step is an assessment of your current environment. What needs improving? What are Security's fixed conditions? What recent changes have impacted Security, such as new business directions, new stakeholders, or a merger or acquisition?

DEFINE RISKS & DESIRED OUTCOME 02

An SEC team made up of former CSOs will engage with you to identify the key risks and determine the continuum of desired outcomes depending on your conditions. We map the solution to your C4R – current circumstances, conditions, culture and resources.

SEC RESEARCH & KNOWLEDGE BASE ANALYSIS 03

Once we understand the issues and potential barriers, we search our extensive security knowledge base for resources or research data that can be used as a base or to kickstart direction ideas.

COLLECTIVE KNOWLEDGE™ REVIEW 04

Next, our subject matter experts bring their varied experiences and knowledge together to create a plan to help you reach your desired outcome. We call this Collective Knowledge™.

05 EXAMINE & ALIGN FOR UNIFIED RISK

We help determine which other functions the plan should touch and align with. We use the SEC's Unified Risk Oversight™ model to help plan and communicate the value of cross-functional collaboration.

06 SPONSORSHIP ACCEPTANCE & EXECUTIVE VALIDATION

We assist in communicating the value of the project to the business leader accountable for Security's new vision. This in turn assists in communicating the strategy to senior executives from other functions.

07 DEFINE BUSINESS VALUE MEASURES

Business value metrics are developed for the client team to measure and determine project success for the organization, including key stakeholders.

08 IMPLEMENTATION ASSISTANCE

Last, clients can either take the SEC deliverables and run with them, or we can guide you through the implementation of your plan. At the end of the day, **the SEC is here to help you succeed.**

The SEC Process Outcome: Security Leader and Program Success

Elsevier
225 Wyman Street, Waltham, MA, 02451, USA
The Boulevard, Langford Lane, Kidlington, Oxford, OX5 1GB, UK

Originally published by the Security Executive Council in 2006.

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods or professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information or methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data
Campbell, George, 1942-
Measures and metrics in corporate security / George K. Campbell. -- Second edition.
pages cm
"Originally published by the Security Executive Council in 2006."
Includes bibliographical references and index.
ISBN 978-0-12-800688-7 (alk. paper)
1. Corporations--Security measures. 2. Business enterprises--Security measures. 3. Security systems--Management. I. Title.
HD61.5.C363 2014
658.4'7--dc23
2014005929

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-0-12-800688-7

This book has been manufactured using Print On Demand technology. Each copy is produced to order and is limited to black ink. The online version of this book will show color figures where appropriate.

Contents

About the Author

George Campbell served until 2002 as the chief security officer at Fidelity Investments, the largest mutual fund company in the United States with more than $2 trillion in customer assets and 32,500 employees. Under Campbell's leadership, the global corporate security organization delivered a wide range of proprietary services including information security, disaster recovery planning and crisis management, criminal investigations, fraud prevention, and more. Since leaving Fidelity, Campbell has served as a content expert for the Security Executive Council, of which he is a founding Emeritus Faculty member.

Prior to working at Fidelity Investments, Campbell owned a security and consulting firm, which specialized in risk assessment and security program management. He has also been group vice president at a system engineering firm that supported government security programs at high-threat sites around the world. Early on in his career, Campbell worked in the criminal justice system, and served in various line and senior management positions within federal, state, and local government agencies.

Campbell received his bachelor's degree in police administration from American University in Washington, DC. He served on the Board of Directors of the International Security Management Association (ISMA), and as ISMA's president in 2003. Campbell is also a long-time member of ASIS International. He is a former member of the National Council on Crime Prevention, the High Technology Crime Investigation Association, and the Association of Certified Fraud Examiners, and is an alumnus of the US State Department's Overseas Security Advisory Council.

Introduction

Over the past several years, the more I have worked with some really good security organizations to assess and develop their metrics programs, the more I am convinced that metrics is not about the numbers, it is about measuring performance of people, process, and performance. Do not get me wrong, we need to build and maintain lists of numbers, but this is just the beginning of the work. Like a smart colleague of mine says, "It's just counting nails." What do these numbers mean? What story do they tell, what action is required and by whom?

Much of what follows in this book is focused on examples of security management challenges and opportunities and the role and contribution I see for measurements and metrics. But I think it is important to level set where you stand in terms of your program's status whether you are reading this as a security executive with a solid metrics program, some one desiring to reinvent or build a body of security metrics or perhaps as a student of the discipline. In working with scores of corporate security organizations over the past decade, I have found that there are about a dozen questions about a security organization's metrics program that effectively serve to focus the manager on developmental priorities. It is a logical beginning to this book and aids in consideration of the potential value of the examples that are discussed throughout.

Metrics program assessment

> What is the business case for your security organization and how do you want it measured? What are the quantifiable measurements that ought to apply to management's assessment of value? How would you grade your measurements and metrics?

The following metrics self-assessment tool walks the security manager through a number of questions about how they would rank their program's maturity. Take an honest look at each of the descriptions and see how you would assess your current security metrics program. If you think carefully about the questions and your assessment compared to the alternatives, I think you will find a road map for targeted improvements.

You can work this assessment on your own if you are a sole practitioner. But if you have a team of managers leading various programs and functions, it would be advisable to develop this as a team exercise. It will get everyone (hopefully) on the same page and likely identify a host of strengths, weaknesses, opportunities, and threats (SWOT). This self-assessment is a precursor to the metrics construction process that takes the reader through six steps in building a program. Use it to leverage your strengths and opportunities and note where each of the steps offers an approach to mitigating your weaknesses and threats.

Review and fill in the attached self-assessment questionnaire. Select the statement that best suits your situation and designate the current level of accomplishment for your selection. For example, if you selected "1.2 Management is beginning to seek performance measures and metrics from security," a Level 1 would indicate you are at the earliest stage of response to this need. If none fit the bill, insert your own selection as noted.

Key Metrics Program Indicators	**Maturity Level**		
1. Organizational Context	**Level 1**	**Level 2**	**Level 3**
1.1 Metrics are an accepted element within selected business operations but have not been requested from security			
1.2 Management is beginning to seek performance measures and metrics from security			
1.3 Performance measures and metrics are a required element of program management			
(Insert your own performance indicator if not listed or adaptable above)			
2. Current Status of Metrics Within the Security Department	**Level 1**	**Level 2**	**Level 3**
2.1 Recognized need and trying to understand best first steps			
2.2 Established objective but just in very early stages of development			
2.3 We have a variety of data and now are moving to identify best approach for desired results			
2.4 We have several focused metrics outputs for targeted constituents but now want to elevate the content and management (or board) targeting			
2.5 We have a well-established program with quality reporting and now desire to develop a more directed and influential set of measures and metrics			
(Insert your own performance indicator if not listed or adaptable above)			
3. Data Availability	**Level 1**	**Level 2**	**Level 3**
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			

Key Metrics Program Indicators	Maturity Level		
(Insert your own performance indicator if not listed or adaptable above)			
4. Data Reliability	**Level 1**	**Level 2**	**Level 3**
4.1 Our incident and performance-related data do not currently have consistent standards of review and reliability			
4.2 Although our incident and performance-related data are distributed among multiple organizational units, there are consistent standards of review and reliability for reporting up			
4.3 We have an enterprise-wide incident and performance-related data repository with consistent standards of review and reliability			
(Insert your own performance indicator if not listed or adaptable above)			
5. Analytical Scope and Discipline	**Level 1**	**Level 2**	**Level 3**
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 Selected security programs have established performance measurement criteria and are consistently tracked and subjected to in-depth analysis			
5.4 All security programs are subjected to ongoing qualitative and quantitative measurement with metrics outputs available for management reporting			
(Insert your own performance indicator if not listed or adaptable above)			
6. Analytical Benefits	**Level 1**	**Level 2**	**Level 3**
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 analyses provide evidence of compliance with applicable regulations			
6.4 Our analyses provide evidence of business unit compliance with policies related to internal controls and security			

Continued

—cont'd

Key Metrics Program Indicators	Maturity Level		
6.5 Our analyses of security program performance has enabled demonstrably improved management understanding of the value of security investments			
6.6 Our ongoing analyses of risk assessment and security program performance data are a required deliverable to senior management (and the board)			
(Insert your own performance indicator if not listed or adaptable above)			
7. Reporting	**Level 1**	**Level 2**	**Level 3**
7.1 Reporting is primarily for internal security department program performance tracking			
7.2 There are multiple security functions with no consolidated metrics reporting			
7.3 Formal reporting of program performance data is limited to a select few key indicators required by management			
7.4 We provide a variety of standardized and tailored metrics reports to management on an established schedule			
(Insert your own performance indicator if not listed or adaptable above)			
8. Directional Performance–Standards and Guidelines	**Level 1**	**Level 2**	**Level 3**
8.1 We have not found a set of security-related standards or guidelines that may be useful as measurement benchmarks			
8.2 We currently do no employ an established body of industry or locally developed performance standards or guidelines that may be used as benchmark targets for metrics			
8.3 We have adopted a selected set of measurable performance standards or guidelines developed by others that are tracked and reported to management			
8.4 We have both adopted externally produced performance standards and developed others appropriate to our unique business management requirements			

Key Metrics Program Indicators	Maturity Level		
(Insert your own performance indicator if not listed or adaptable above)			
9. Actionability	**Level 1**	**Level 2**	**Level 3**
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			
(Insert your own performance indicator if not listed or adaptable above)			
10. Resources and Tools	**Level 1**	**Level 2**	**Level 3**
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			
10.4 Our company has developed dashboard models that we are adapting to suit our security metrics reporting requirements			
(Insert your own performance indicator if not listed or adaptable above)			
11. Data Sensitivity and Protection	**Level 1**	**Level 2**	**Level 3**
11.1 There are safeguards that protect the confidentiality of metrics data that could reveal potentially risky information to unauthorized individuals			
(Insert your own performance indicator if not listed or adaptable above)			
12. Summary Assessment–Measuring Security's Value to the Enterprise	**Level 1**	**Level 2**	**Level 3**
12.1 We are actively seeking a body of metrics capable of demonstrating measurable value to the enterprise			
12.2 We have a body of metrics accepted by management as demonstrating measurable value to the enterprise			

Continued

—cont'd

Key Metrics Program Indicators	Maturity Level
(Insert your own performance indicator if not listed or adaptable above) Organization: Evaluator: Date:	

Using this assessment

If you are just beginning this hunt for your few meaningful metrics, you need to carefully consider the implications of your choices. For example, consider your selection of these options:

3.1 We do not currently have a centralized incident reporting system;
4.1 Our incident and performance-related data do not currently have consistent standards of review and reliability; and
5.1 Current processing of incident and performance data is primarily limited to maintaining counts of various data elements for trend analysis and reporting.

The absence of a centralized reporting system is not a show-stopper but the lack of an effective incident reporting system is. In the former, you have the data spread among various entities but it will be more difficult to bring it into a form that enables solid analysis. In the latter, you likely cannot rely on the data it is going to be difficult to even gather; thus the likely selection of 4.1. When you have the data and you are confident of its accuracy, remember that after you put it in a form that essentially enables counting, that is only the beginning. Counts are okay for trending but do not provide direction for alternative action; they merely serve up the fuel for your analysis and decisions.

Reliability is the heart of a metrics program so that is your first priority in the building process.

Every one of these assessment items has its own implications for your next steps. If you are alone in interpreting your results or the team needs some thoughtful advice, think about the short story above and find a mentor who can help you sort the options and be a supporter in the construction process. If you are in great shape, check out the examples and hopefully find a number of ideas for adding and improving your security metrics portfolio.

Building your program

If you have come away from the assessment with a conclusion that you have a mature, well functioning metrics program that is delivering measurable results to you as a manager and to your customers, I suggest you use the table of contents to

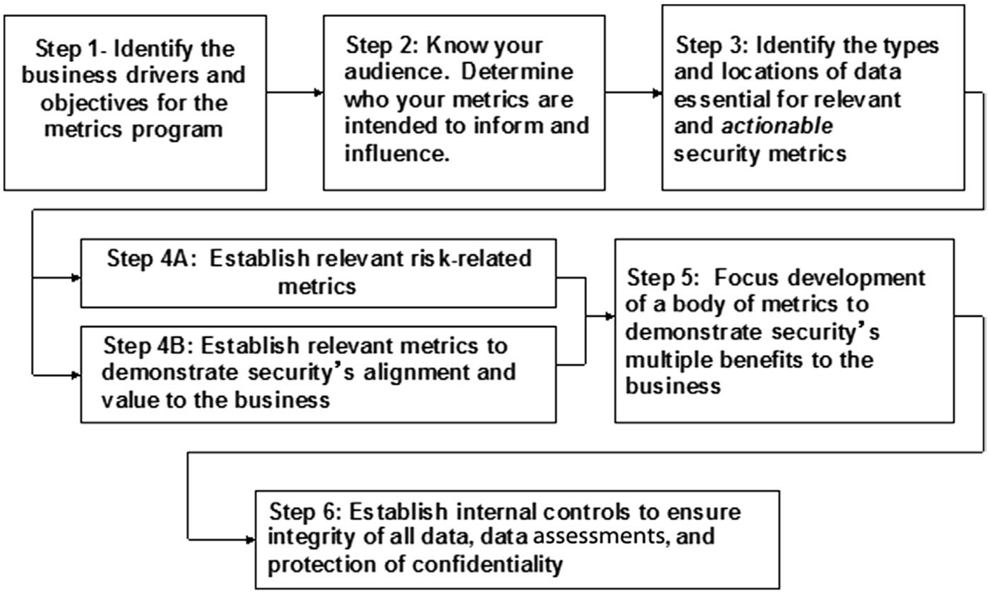

Step 1- Identify the business drivers and objectives for the metrics program
Step 2: Know your audience. Determine who your metrics are intended to inform and influence.
Step 3: Identify the types and locations of data essential for relevant and *actionable* security metrics
Step 4A: Establish relevant risk-related metrics
Step 4B: Establish relevant metrics to demonstrate security's alignment and value to the business
Step 5: Focus development of a body of metrics to demonstrate security's multiple benefits to the business
Step 6: Establish internal controls to ensure integrity of all data, data assessments, and protection of confidentiality

FIGURE 1

Construction process for implementing a security measures and metrics program.

cherry pick topics that I hope will deliver an actionable idea or two. If the assessment helped you focus on some gaps or shortcomings or if you are engaged in a bottoms-up reinvention, perhaps a review of the following (Figure 1) will find an approach to set your program in the right direction.

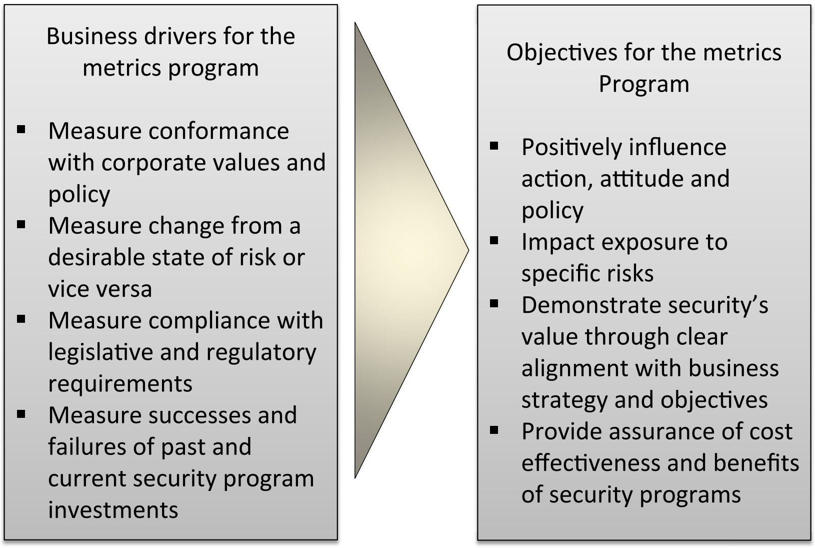
Step 1: Identify the business drivers and objectives for the security metrics program

Where can metrics deliver the greatest benefits for your company and the security mission?

- Is to make a positive impact on company policy and culture?
- Or should it be to measurably impact risk exposure?
- How about to demonstrate security's alignment with business goals and bringing value to the bottom line?
- How about all of these and more?

Look at the key words in Figure 2: risk, measure, value, policy, influence, impact, change, compliance, alignment, and strategy. These are the high profile targets of your metrics.

Be clear on your priorities and objectives as you begin to develop your program. Talk to your boss and probe what management would value and how they would use actionable metrics from your organization. Learn who of your colleagues is measuring and reporting with quality and relevance. I will give you a tip that your information security partner has volumes of established metrics you can use as a model.



Business drivers for the metrics program

- Measure conformance with corporate values and policy
- Measure change from a desirable state of risk or vice versa
- Measure compliance with legislative and regulatory requirements
- Measure successes and failures of past and current security program investments

Objectives for the metrics Program

- Positively influence action, attitude and policy
- Impact exposure to specific risks
- Demonstrate security's value through clear alignment with business strategy and objectives
- Provide assurance of cost effectiveness and benefits of security programs

FIGURE 2

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

Do not take this step lightly. Create a formal process for identifying what management wants and needs. Think about the knowledge resident in your programs that offer quality guidance to business strategy and an improved state of risk management. There is a clear correlation between how well you identify these needs and how successful your program will be.

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

You are well aware of what will happen if your company fails to connect with the needs of its customers. I cannot overemphasize the importance of understanding the diversity of perceptions about risk and how each of your constituents view your role in its management. Metrics are central to our ability to influence and engage our customers in their role in corporate security and brand protection. They enable a coherent set of messages focused on a targeted audience.

Each of these audiences (see Figure 3) has a unique agenda and set of needs, a "hot button," if you will. Some need to see the broader view with a clear assessment of alternatives. Others require the 10 min laser approach to the problem and best solution. You must know your customer and what motivates them to action. Your message has to be tailored to influence, to enable them to see why your message deserves their acceptance and buy-in.

Metrics should be presented as enabling tools rather than criticisms whenever possible. Positive action is more likely if the audience feels he or she is being given an opportunity rather than a sharp stick in the eye. You want partnership in results more than a notch on the gun.