Security Leadership Solutions
Executive Council

Security Executive Council Publication Series

MEASURES and METRICS In CORPORATE SECURITY:

- *HUNDREDS OF PROVEN MEASURES AND METRICS*
- *TOOLS TO DEMONSTRATE THE EFFECTIVENESS OF YOUR SECURITY PROGRAM*
- *WORKBOOK FORMAT*

by

George K. Campbell

ABOUT THIS PUBLICATION

MEASURES and METRICS in CORPORATE SECURITY
A Value Initiative Product: A Workbook for Demonstrating How Security adds Value to Business

George K. Campbell, Security Executive Council Emeritus Faculty Member and former Chief Security Officer at Fidelity Investments is author of the ground-breaking book, *MEASURES and METRICS in CORPORATE SECURITY* The risk environment has changed significantly over the past 30 years with shocking wake-up calls to CEOs, Boards and shareholders. Campbell, an industry leader with over 30 years of executive-level security experience, leads a discussion on the surprising range of security measures and metrics options, deciding on the most significant data and how best, and to whom, to present it. This is a workbook intended to stimulate thought on what might be effective within your unique environment and guides the reader to develop their metrics program. ***Measures and Metrics*** is more than a "how to"; it's about managing the security organization and aligning it with the business goals. With a background covering information security, disaster recovery planning, due diligence, criminal investigations, fraud prevention, property protection and security systems engineering, Campbell comes well-equipped to discuss the metrics and measurements that make up a successful security program. In this book he puts forth solid answers to the question, "Why security metrics?" At the same time he provides examples for addressing company-wide security concerns. This book contains useful information for both the public and private sectors, the new and experienced CSO, CISO, risk manager, auditor or executive with security responsibility as well as MBA and advanced security degree students.

Reserve your copy of *Measures and Metrics in Corporate Security* today at http://www.securityexecutivecouncil.com

Intended Audiences:

- Security Professionals
- Compliance Professionals
- Corporate General Counsel
- Sr. Corporate Executives
- Internal and External Auditors
- Ethics Officers
- Risk Management Professionals
- College-level Professors/Instructors of Security-related Curricula
- Students

TABLE OF CONTENTS

George Campbell is currently a member of the Emeritus Faculty of the Security Executive Council. He retired in 2002 as Chief Security Officer at Fidelity Investments, the world's largest privately owned financial services firm. Under George's leadership, the global corporate security organization delivered a wide range of proprietary services including information security, disaster recovery planning, background, due diligence and criminal investigations, fraud prevention, property protection and security system engineering. During the period 1989-92 George owned his own security-consulting firm and from 1978-89 was Group Vice President at a system engineering firm supporting worldwide U.S. Government security programs. His criminal justice career from 1965 to 1978 was spent in various line and senior management functions within federal, state and local government agencies.

George received his baccalaureate degree (Police Administration) from American University, Washington, D.C. in 1965. He is a Life Member and served on the Board of Directors of the International Security Management Association from 1998-2003 and as ISMA's President in 2002-03. George is a member the American Society for Industrial Security since 1978. He is former member of the High Technology Crime Investigation Association, the Association of Certified Fraud Examiners and an alumnus of the U.S. Department of State, Overseas Security Advisory Council.

1. THE BASICS

1.1 Introduction. Corporate security organizations have long sought a catalog of metrics or measures that may be applied to reliably indicate the value they bring to the enterprise they serve. While easily focusing on the company's quarterly earnings, department budget runs and certain incident statistics, many corporate security managers fail to utilize the volumes of data their operations generate that may be organized to provide a rich array of performance assessment tools.

This book is intended to provide some organizational measurements, concepts, metrics, indicators and other criteria that may be employed to structure measures and metrics program models appropriate to the reader's specific operations and corporate sensitivities. This is a workbook, and a work in progress, intended to stimulate thought on what might be effective within your unique environment. We briefly touch on multiple measures and metrics because there are so many alternatives and the workbook format may enable you to find one example that can be modified to accommodate your needs better than another. We need to share these ideas and hopefully future versions of this workbook will encompass examples of what has worked for you.

Caveat Emptor! Security metrics are not about numbers; they are about performance. Unless you have the intestinal fortitude to adequately plan and execute a program to legitimately measure how well specific security programs are delivering on their objectives -- and stand the heat from the answers you may get -- you likely are not going to benefit from this discussion. But your programs will be measured with or without you. Having the answers is just good management.

1.2 Why Measure, Why Metrics? The fact that established metrics and measures for the full range of security programs are few and far between tells a story about the historical disconnection of these functions from the core businesses they serve. The risk environment has changed significantly over the past 30 years with shocking wake-up calls to CEOs, Boards and shareholders. Attentive corporations have had to address the exposures uncovered in these times with more sophisticated and mainstream corporate security organizations. With this mainstreaming comes the need (obligation) to measure performance and demonstrate contribution to the bottom line. Metrics are a natural descendant of this process.

2. TYPES OF METRICS & PERFORMANCE INDICATORS

2.2 **The CSO Dashboard.** Every CSO should have half a dozen dials that are watched on a regular basis. These indicators could be "survival metrics"-- the hot buttons you are expected to address or those few dials that monitor selected wellness indicators unique to your organization or of particular concern to management. If you are in financial services, you might be particularly attuned to the number of business units with dated contingency plans and inadequate software patch administration, internal misconduct or numbers or people hired with known derogatory backgrounds. Your business may be in hostile locations or increasingly dependent on third parties you know have poor security controls. What if you are concerned that your security service vendor is giving you increasing numbers of problematic personnel? Each of us can select a few key metrics we should watch because they are the things that keep us awake at night. You may find that you have more than one dashboard -- yours and the one(s) your boss and a few key others expect you to watch and report on. The CFO may be an excellent resource to advise on the presentation of dashboard metrics since this officer typically reports performance metrics to management on a regular basis.

Look for some meters or dials in the following discussions that can serve to improve or develop your dashboard.

🟥 **SECURITY COST**	**Security cost per dollar of revenue is up past two quarters**
🟥 **INFO SECURITY**	**14% decrease Q2 vs. Q1 in devices with appropriate patches installed and current**
🟨 **BUSINESS CONDUCT**	**Year-to-date investigative results indicate 20% increase in non-compliance with business conduct policies**
🟩 **SECURITY AUDITS**	**100% of all notable security-related audit findings have been successfully resolved**
🟩 **PRE-HIRE Backgrounds**	**55% of all new hires have completed & resolved background investigations**
🟨 **BUSINESS CONTINUITY**	**17% of critical business processes do not have up-to-date & tested response plans**

APPENDIX 1: Examples of Security-Related Measures and Metrics

The following tables are not intended to provide a comprehensive inventory of security-related measurements and metrics. It is proposed as a prompt to stimulate thought, debate and discussion appropriate to the unique organizational setting and purposes for which they will be utilized in your application. Many have been used in actual practice and have proven validity. You should not take them as-is without truly making them relevant to your organization and what is important to your constituents. *These are starting points.*

The reader is encouraged to focus on developing a measures and metrics program that serves core business objectives, supports proactive risk management and enables real assessment of the effectiveness and value of security programs and processes.

The tables in each of the following sections are organized to enable the reader to assign each selected measure or metric to an associated business driver in the following sample fashion.

EXAMPLE							
SECURITY MEASURE OR METRIC	**BUSINESS DRIVERS**						
	COST MGT.	**RISK MGT.**	**ROI, VALUE**	**LEGAL REQ.**	**POLICY REQ.**	**LIFE SAFETY**	**INTERNAL INFLUENCE**
The number of nuisance alarms from corporate facilities monitored by Corporate Security	**X**	**X**				**X**	
Security cost as a percentage of total company revenue	**X**		**X**				
The number of safety hazards proactively identified and eliminated annually		**X**		**X**	**X**	**X**	
Percentage of critical information assets or functions residing on systems that are currently in compliance with approved system architecture		**X**			**X**		**X**
The number of failed or ineffectual business unit responses to issues identified by Security as control weaknesses that result from fraud prevention analysis, investigations or other feedback		**X**					**X**

It is hoped that the results of this approach will assist the CSO in focusing on the selection of specific measures or metrics that best serve the demonstration of business responsiveness and perceived value.

Hundreds of examples are provided; categories include:

- Security Related Trends - General
- Communicating Risk Knowledge
- Audit Implications
- Background Investigations
- Due Diligence Examinations
- Business Conduct & Reputational Risk
- Criminal Incidents and Investigations
- Security Operations, Physical Security & Premises Protection

- Informational Risk Management
- Contingency Planning & Business Continuity
- Business-based Security Programs
- Confidence with the Corporate Security Functions
- Management, Professional Development & Employee Satisfaction

This workbook is intended to grow as readers submit their examples and best received security-related measures and metrics.

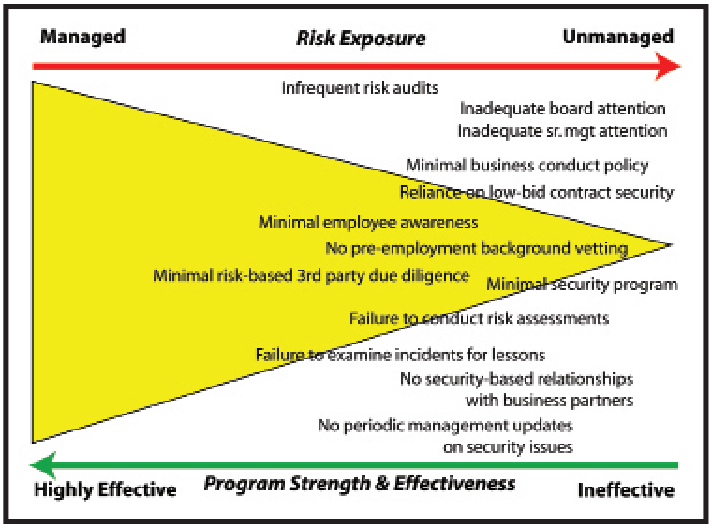
Following are a sample of reprints
from George Campbell’s
Security Technology Executive magazine
column entitled
Metrics for Success
that demonstrate using the metrics
described in this book.

Threat Assessment: Measuring Likelihood

By George Campbell

When you think about security threats to your business, which do you think are likely to manifest? What are the probabilities of a specific type of event occurring at a particular location? How do you convey your concerns to management without sounding like Chicken Little yelling that the sky is falling? It is essential that we keep our eye on "what if." In the security mission, we operate the radar. We possess unique knowledge and perspective on business risk. We have a responsibility to view the risk landscape and scope out the trends, the behaviors and the gaps in common-sense protection and then select the targets and style of our alerts.

Strategy: Risk assessment clearly involves a threat assessment component, and event likelihood is a critical element. We may view likelihood in a variety of analytical ways, but I like to look at it as the degree to which our exposure to various risks is managed by the strength and effectiveness of our internal controls and security measures. There are scores of factors or measures that might be employed given your company's business risk environment and the scope of its security program, but here are a few to consider.


Managed
Risk Exposure
Unmanaged
Infrequent risk audits
Inadequate board attention
Inadequate sr. mgt attention
Minimal business conduct policy
Reliance on low-bid contract security
Minimal employee awareness
No pre-employment background vetting
Minimal risk-based 3rd party due diligence
Minimal security program
Failure to conduct risk assessments
Failure to examine incidents for lessons
No security-based relationships with business partners
No periodic management updates on security issues
Highly Effective
Program Strength & Effectiveness
Ineffective

- The degree to which management supports the establishment and communication of policy and expectations on conduct and security-related responsibilities:
  - Security issues are on Board agendas as required.
  - Management requires ownership of business unit role(s) in security measures.
  - Business conduct policy is in place and supported by action.
  - Background investigation standards are in place and followed in the hiring process.
  - Security is regularly on senior management's agenda and takes ownership for supporting corrective actions as required.
  - Management demands timely identification and escalation of issues.
- The degree to which we elect to probe security measure effectiveness:
  - There is a routine for focused risk assessments and internal control audits.
  - There is a routine for tests of security plans and required follow-up actions.
  - There is a routine for targeted incident post mortems and lessons-learned exercises.
  - Employees' awareness of their role in protection is periodically reinforced.
  - Outsourced partners with access to critical business processes or assets are vetted for their commitment to the protection of our brand.
- The degree to which security resources are maintained at a high degree of competency and responsiveness:
  - The security program is clearly established as an equal element of the corporate risk management infrastructure.
  - Security responsibilities are clearly articulated and personnel are held to high standards of performance.
  - Security objectives are clearly linked to a risk management strategy and plan.
  - Contractors are selected and evaluated on standards of performance rather than just low bid.

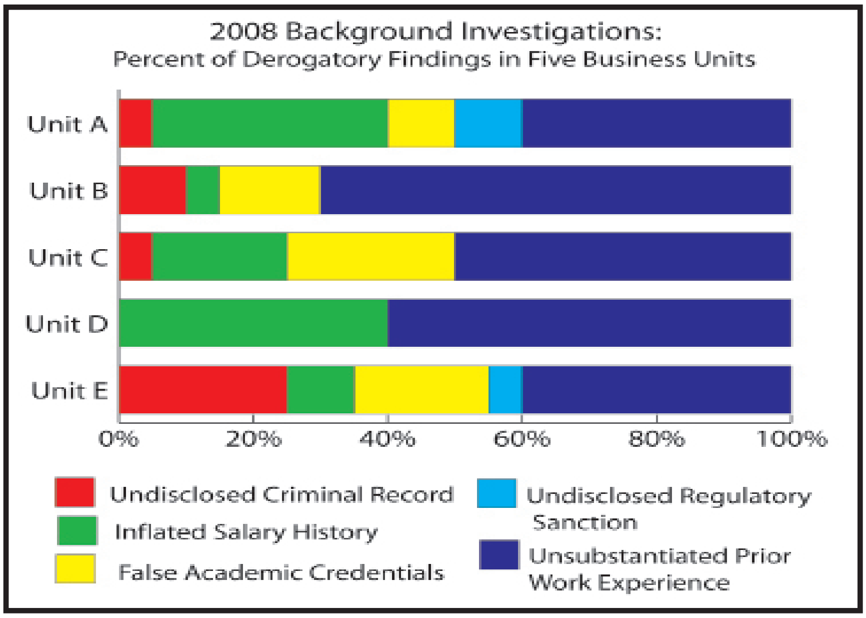
You can construct this list of in any number of ways to be consistent with the scope of your security program(s). My list here tends to accentuate the positive, but you could easily list your assessment of the apparent gaps and program shortcomings, as does the figure above. This picture engages senior management's attention, and its serious tone demands a level of verifiable audit and risk assessment findings.

We know that likelihood of risk is influenced by the weakness or absence of safeguards. We need to tell stories to management that eliminate plausible denial, establish accountability, and influence policy and action. A presentation like this connects the dots by showing how the combination of control weaknesses demonstrates an increased potential for business and reputational risk. ■

George Campbell is emeritus faculty of the Security Executive Council (SEC) and former CSO of Fidelity Investments. His book, "Measures and Metrics in Corporate Security," may be purchased through the SEC Web site. The SEC is a risk mitigation research and services organization for senior security and risk executives from corporations and government agencies responsible for corporate and/or IT security programs. For more information about the Council, visit www.securityexecutivecouncil.com/?sourceCode=std.

Demonstrate a Need for Stronger Background Vetting

By George Campbell



A comprehensive background investigation program is critical to the health and integrity of any enterprise — in good times and especially in bad. A worsening of the economy can have a striking impact on the honesty of the employee candidate pool, and it can also affect the quality of internal and external background vetting.

Objective: We need to demonstrate to management and HR the impact of the current recession on background investigations and their results, in order to urge greater due diligence in the selection process.

Strategy: If we look at business contraction from our unique perspective of enterprise risk, we will see several potential implications:

- When the business is doing poorly and hiring has stopped or slowed, hiring managers may seek to be exempted from hiring freezes by citing a critical need for an essential position. They may exert pressure to lower investigation standards to streamline the process on new hires, and they may overlook blemishes they would find undesirable in more competitive times.
- Outsource providers may push back on contractual requirements for background investigations altogether or attempt to impose their own less-stringent standards of selection.
- Even in the best of times, headhunter agencies encourage creative writing and embellished work experience to maximize their candidates' qualifications. Today's job pool is alive with unemployed professionals being represented by these agencies.
- During recessionary periods like the one in which we now find ourselves, there is strong evidence that the honesty quotient in the employment pool declines and the unemployed may embellish their personal histories and qualifications.

We need to feel confident that our background vetting programs are effectively verifying candidate assertions of prior salary and experience, education, supplementary compensation (bonus, perks, incentives, etc.) and benefits. We need to be tracking the ratio of cases with no derogatory findings against ones with various types of potential disqualifiers, also focusing on the variance between different business units.

The chart above clearly shows some switches that need to be reset with these business units and the HR staffing team. The hiring managers are not effectively probing interviewees on the veracity of their personal histories, and the HR recruiters are simply leaving any semblance of vetting to Security's background investigators. These candidates have fabricated their prior experience to suit the job descriptions and held up the hiring manager by inflating their prior salary history. This picture also should alert the reader who employs outside background investigation vendors to ensure they are getting the truth lest every step in the process would fail.

These trends will tell stories about the level of due diligence being done by HR recruiters, headhunters and hiring managers, and you may need to use this data to reset some switches. You may find data for measuring these trends in your investigative postmortems and employee termination-for-cause statistics.

Stay on top of what your background investigation data is telling you about the candidate pool in your company and for your key vendors, especially those providing services around critical business processes with reputational impact. I'm often struck by the companies I talk to who are not using the basic safeguard of background vetting. If you are one of those, you need to engage senior management on the need. Try telling them that the people you are not screening are the ones that have been rejected by your competitors, who are doing a good job in background reviews. ▮

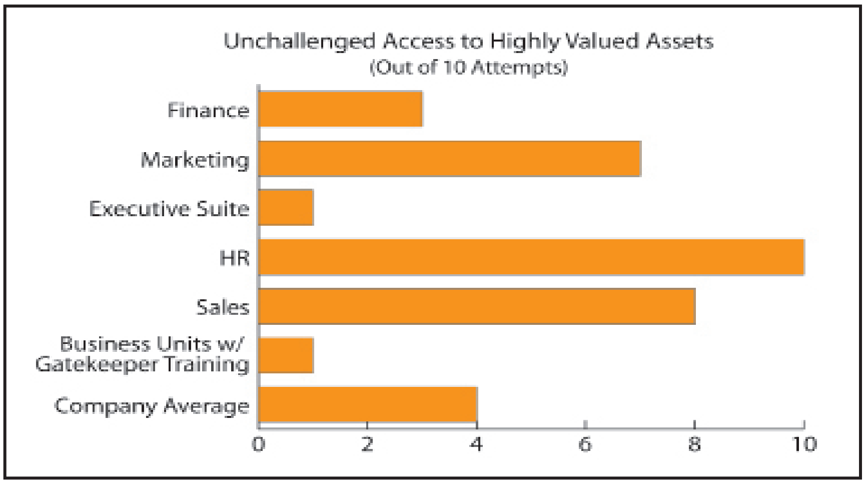
George Campbell is emeritus faculty of the Security Executive Council (SEC) and former CSO of Fidelity Investments. His book, "Measures and Metrics in Corporate Security," may be purchased through the SEC Web site. The SEC is a member organization for senior security and risk executives from corporations and government agencies responsible for corporate and/or IT security programs. In partnership with its research arm, the Security Leadership Research Institute, the Council is dedicated to developing tools to establish security as a value center. For more information, visit www.securityexecutivecouncil.com/?sourceCode=std. The information in this article is copyrighted by the Security Executive Council and reprinted with permission. All rights reserved.

Working with Customers for Better Access Control

By George Campbell

If you have been reading this column each month, you know of my passion for testing and reporting on the effectiveness of the safeguards we have installed to protect our people and assets. You will not influence anyone with metrics that just count things, but you will with ones that really measure how well you and your customers are meeting your responsibilities to protect the company.

Objective: Our intent is behavior modification — not just from our customers, but from ourselves. We may find that we need to take a look at our own ideas about what works and what does not in our protection strategy.



Strategy: If we are serious about our mission, we test safeguards on a regular basis. But we also test them to measure how well they are working and to find soft spots in our strategy. There is no security manager reading this that has not had to deal with a business unit that pushes back and demands "an inviting space and convenience"— translation: unrestricted access involving disablement of electronic or staffed entry controls. Let's think about this for a minute.

How well have we considered the business culture as we have dealt with this "difficult" client? You can bet that for every person openly complaining about security controls, there are more out there who are simply looking the other way when those controls are purposefully bypassed to make life easier for the employees or residents. Any good patrol plan and a cadre of engaged security officers would have already told you which business functions would be targets of opportunity because of such bypasses. In the example above, Security went a step further and conducted 10 unannounced access attempts for each business unit.

If we look at the results of these penetration tests, what might we speculate are the biases of the three bad guys here: marketing, human resources and sales? I do not think I'm generalizing when I state that these functions are typically hard sells for the kind of controls we tend to like. They want convenience and freedom, and we either post someone who challenges entry or install things that impose restrictions.

What should we do with these results? First, let's understand that the findings of these tests revealed access to customer lists, an unsecured CFO Laptop, desktop access via posted password and piggybacking into the computer room by unknown individuals, so it is clear that we have to find ways to improve. We could run to the CEO and drop a dime on the top guys of the Freedom Three, or we could approach each of these managers, discuss what we found, and then find solutions that serve a common ground of enterprise risk management.

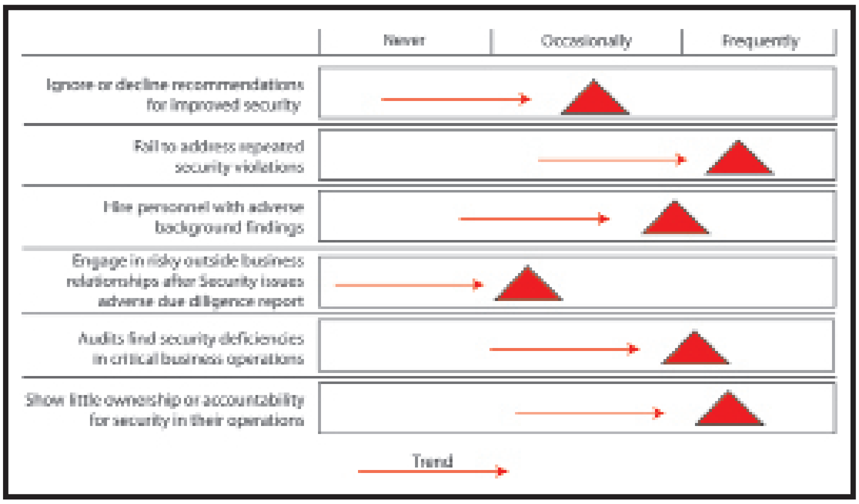
At the end of the day, these senior managers cannot excuse the potential exposures presented by these findings, nor can we in security escape finding more creative and business-compatible asset protection solutions. The security approach we see here is a one-size-fits-all: You have our solution to access control and that's that! Working with each business unit to direct greater protection around tighter, more internal and focused areas where convenience can agreeably give way to expedience is the middle ground found here. I would add that in this case, HR did agree that their exposure to disgruntled and potentially hostile individuals did demand greater access management and control. The model they adopted reflected the lessons from "gatekeeper" risk assessment training for receptionists and assistants coupled with duress-related technology.

Summary: Access management is a core safeguard, but there are a variety of ways to achieve that goal and a variety of user perspectives on how it could best work. Understand the range of risks driving this set of safeguards and work with your customers to tailor the protection strategy for results. ∎

George Campbell is emeritus faculty of the Security Executive Council and former CSO of Fidelity Investments. His book, "Measures and Metrics in Corporate Security," may be purchased through the Security Executive Council Web site. The Security Executive Council is a member organization for senior security and risk executives from corporations and government agencies responsible for corporate and/or IT security programs. In partnership with its research arm, the Security Leadership Research Institute, the Council is dedicated to developing tools that help lower the cost of members' programs, making program development more efficient and establishing security as a recognized value center. For more information and inquiries on membership requirements, visit www.securityexecutivecouncil.com/?sourceCode=std. The information in this article is copyrighted by the Security Executive Council and reprinted with permission. All rights reserved.

Do Business Units Value Security Recommendations?

By George Campbell



Our ability to influence internal customers starts and ends with their perception of the effectiveness and value of security programs. We have to test this perception on a periodic basis, because the results provide opportunities to consider the effectiveness of our programs and alternative approaches to both risk and relationship management.

Objective: An obvious way to track customer confidence is to look at whether business units are accepting Security's recommendations in key areas. In the example from which the graph above is drawn, the Security Director has been tracking several program criteria that should be valid indicators of Security's perceived credibility.

There's a little good news and a lot of bad in these results. The good news is that there is a program to track results in several core areas. The bad news is that there seems to be a dramatic disconnect between security and the rest of the business.

First, there is a consistent set of adverse trends across the range of programs. Next, these findings may indicate more fundamental exposures to corporate risk that are not being effectively mitigated by established security measures, and that points to weakness in the Security Director's leadership. Finally, I have to conclude that senior company management has failed to communicate that they expect business units to play a role in brand protection and corporate integrity. This is clearly impacting the Security Director's ability to lead and influence results.

Consider these findings:

1. Business units ignore or decline recommendations for improved security *occasionally, but trending up.* This is about as basic a measure as you can find. You have delivered multiple recommendations to address security gaps, but your findings have had a minimal impact on the state of protection. Did the business fail to connect the findings to real business risk? Security needs to take a hard look at the quality of its findings and presentation. They should also consider a new approach to visibly escalating non-compliance.

2. They fail to address repeated security violations *increasingly frequently.* If this company had any sense of the relationship of security risk to corporate risk, this would be on the audit committee agenda. This result clearly shows the Security Director's failure to lead and influence with the facts, exacerbated by an unsupportive tone at the top.

3. They hire personnel with adverse background findings *occasionally, but trending up.* Business units do not know how to relate a bad background to a potential risk in their midst. Security has not adequately communicated the consequences of hiring people who have not been truthful in the process. The Director needs to engage with his counterpart in Human Resources to validate this program. Here is another area where Security should be helping senior management to connect the dots.

4. They engage in risky outside business relationships after Security has issued an adverse due diligence report *infrequently, but trending up.* Security is showing the business that there are risks in a proposed relationship, but they choose to partner anyway. The business doesn't get it, so Security needs to work with Audit to maintain a risk watch on these outsourced operations.

5. There are notable audit findings with regard to security deficiencies in critical business operations *frequently, and trending up.* This is a clear and independent assessment that reinforces a failure in the status of corporate governance and security management leadership.

6. Business units show little ownership or accountability for security in their operations *frequently, trending up.* An obvious conclusion of significant shortcomings in the objective of shared responsibility for asset protection.

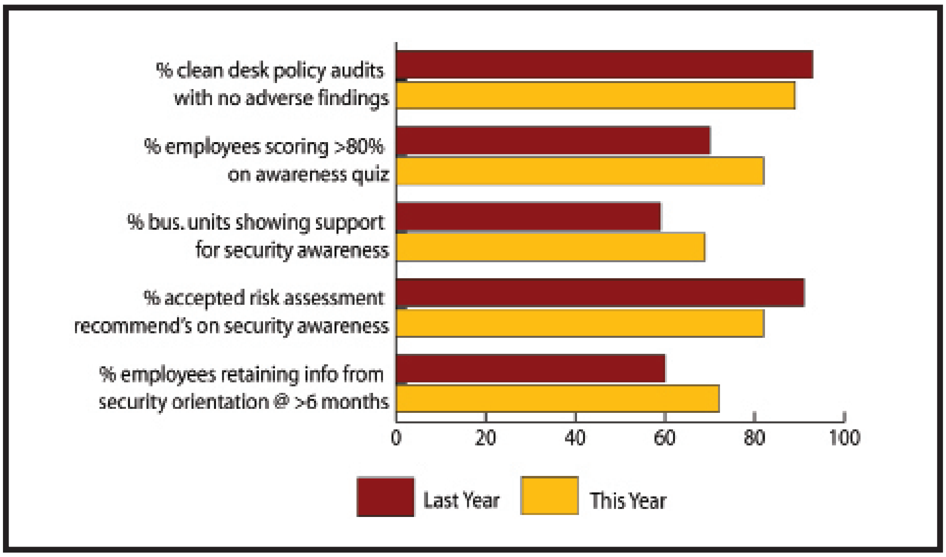
Is this quarterly assessment a reflection of totally inadequate security management or an indictment of this company's senior leadership's failure to provide the Security Director with a clear charter and mandate to impact corporate policy and behavior? Perhaps it is a combination of both. Remember that this is an ongoing assessment process.

What would you do to turn this company around on these performance indicators? ▮

George Campbell is emeritus faculty of the Security Executive Council (SEC) and former CSO of Fidelity Investments. His book, "Measures and Metrics in Corporate Security," may be purchased through the SEC Web site. The SEC is a risk mitigation research and services organization for senior security and risk executives dedicated to developing tools that help lower the cost of security programs, making program development more efficient and establishing security as a recognized value center. Visit www.securityexecutivecouncil.com/?sourceCode=std. The information in this article is copyrighted by the SEC and reprinted with permission.

Security Awareness: A Few Key Indicators

By George Campbell



Security's ability to educate and empower their customers in their risk management responsibilities is a fundamental element of any business protection strategy.

Objectives: To develop a multi-dimensional security awareness program that incorporates a marketing and communication strategy focused on key areas of employee safety, corporate integrity and business process security and resiliency. To identify relevant areas of risk awareness that the targeted population should address.

Strategy: If your company thinks Security is the owner of security-related business risk, get your résumé up to date! We are paid to understand the range and depth of risks confronting the business in its various environments, to build strategies to mitigate them, and to educate our constituents on their responsibilities. Business process owners' awareness is a fundamental element in a security risk mitigation strategy.

If you expect key individuals and groups to conform to policy and procedures, you must use focused communication to ensure that they are aware of those requirements. So, what is Security's brand at your company and to whom do you sell it? Think about it. You have products to sell to senior management, the Board, employees, partners, vendors and visitors. What is your tagline — your brand that guides and frames the message for your constituents? How are you "selling" accountability for business protection?

We have to craft messages that connect in actionable ways with the individuals and organizations responsible for business process integrity and continuity. Your unique knowledge of and perspective on business and personal risk is the raw material you must use to design your mix of products and services. The challenge is to determine what risk management knowledge has to be passed on to whom. Seek out advice from your company marketing and communications departments. They can point your messages in highly productive directions.

Security awareness is measurable. Actionable measures and metrics for risk awareness may be derived from a variety of sources:

- Risk assessment findings provide qualitative data that needs to be fed back to appropriate business units to make them more aware of their accountability.
- Risk events and profiles identify unmanaged exposures that need to be communicated. You can determine the absence or degree of measureable improvement in risk exposure or conformance to policy by conducting follow-up testing of your awareness initiative to see how well the messages got across.
- Formal feedback surveys and interviews can identify the level of security awareness within targeted populations. A useful technique is to use the corporate intranet to quiz users and engage in random polling on risk or procedural responsibilities.
- Incident post mortems, lessons learned and victim interviews provide a rich source of information on gaps in security awareness.
- Security department customer satisfaction surveys can ask how well respondents understand Security's messaging and how effective the communication media is.
- Policy audits, such as clean desk policy checks performed by evening shift security officers during rounds.

The graphic above provides several simple examples of key security awareness indicators. By using percentages of movement over time, you can easily measure improvement or decline. Do not neglect to measure the level of support that business unit management shows for awareness initiatives and corrective actions resulting from risk assessments.

Corporate security and brand protection is every employee's job. The quality of your connection — your actionable messages — with them is a key element of security management. ▮

George Campbell is emeritus faculty of the Security Executive Council (SEC) and former CSO of Fidelity Investments. His book, "Measures and Metrics in Corporate Security," may be purchased through the SEC Web site. The SEC is a research and services organization that involves a range of risk management decision makers. Its community includes forward-thinking practitioners, agencies, universities, NGOs, innovative solution providers, media companies and industry groups. Backed by a Faculty of more than 100 successful current and former security executives, the Council creates groundbreaking Collective Knowledge research, which is used as an essential foundation for its deliverables. For more information about the Council, visit www.securityexecutivecouncil.com/?sourceCode=std. The information in this article is copyrighted by the SEC and reprinted with permission. All rights reserved.

A Solution Provider for Managing Business Risk

The Council develops proven practices that provide an array of strategies and tactics to solve pressing issues based on your situation. With a Faculty of more than 100 successful experienced security executives we work one-on-one with Tier 1 Security Leaders™ to help them reduce risk and add to corporate profitability in the process. Through our pioneering approach of Collective Knowledge™ we serve businesses from all industries and sizes, government agencies, educational institutions and NGOs to help them effectively address their risk concerns. The Council can help you with your security concerns or challenges.

Contact:	Bob Hayes, Managing Director
Web:	www.securityexecutivecouncil.com
Phone:	202.730.9981
E-mail:	contact@secleader.com