ELSEVIER

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

Elsevier
Radarweg 29, PO Box 211, 1000 AE Amsterdam, Netherlands
The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, UK
225 Wyman Street, Waltham, MA 02451, USA

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, 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, 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.

ISBN: 978-0-12-802841-4

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

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

For Information on all Elsevier publications visit our website at http://store.elsevier.com/SecurityExecutiveCouncil

SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Sharing is Caring: Measuring and Communicating Security's Value

This book builds on George Campbell's Measures and Metrics in Corporate Security. While Measures and Metrics guides you through creating a meaningful security metrics program, Measuring and Communicating Security's Value takes you to the next step: using the metrics you deliver to communicate quantifiable value to the organization.

The book includes metrics, key performance indicators, and key risk indicators that have been used effectively in other companies; a detailed program assessment; and information on where to find data and how to use it to create a compelling visual. It demonstrates how to improve influence and how to measure it, how to measure the impact of incidents, how to use metrics to influence policy, and more.

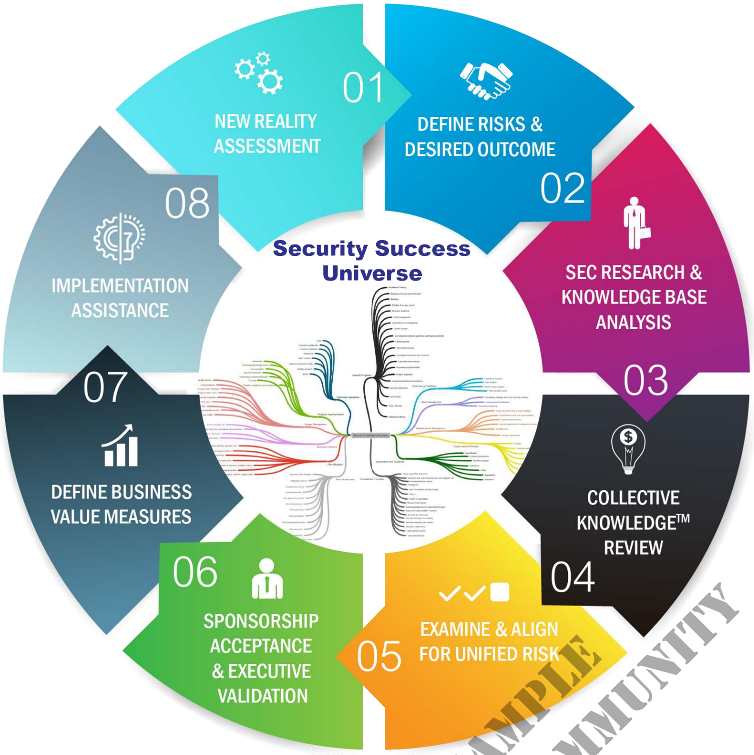
Ways to use this resource:

- To broaden the metrics program by discovering new metrics you may not have considered
- To learn how to effectively present metrics in a meaningful way
- To assess your existing metrics program for improvement
- To enhance the influence of your program

Send feedback about this resource to: contact@secleader.com

THE SEC PROCESS

We walk clients through eight critical steps to reach their goals



01 NEW REALITY ASSESSMENT

02 DEFINE RISKS & DESIRED OUTCOME

03 SEC RESEARCH & KNOWLEDGE BASE ANALYSIS

04 COLLECTIVE KNOWLEDGE™ REVIEW

05 EXAMINE & ALIGN FOR UNIFIED RISK

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

Contents

About the Author

George Campbell has served as a member of the Emeritus Faculty of the Security Executive Council (SEC) from day 1. In addition to consulting activities with the SEC, he has focused his research and development on corporate security performance measures and metrics. 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 the full range of proprietary security risk management services. He previously owned his own security consulting firm and was the Group Vice President at a system engineering firm supporting high security US Government security programs from 1978 to 1989. His criminal justice career from 1965 to 1978 was spent in various line and senior management assignments within federal, state, and local government agencies.

He is a member of ASIS International since 1978 and a frequent speaker and contributor to professional security journals and seminars. He is the coauthor of the *ASIS International Chief Security Officer Standard for Organizations*, author of *Measures and Metrics in Corporate Security* published in 2005, and contributing editor of *Adding Business Value by Managing Security Risks* published in 2009 by the SEC. He was the 2006 CSO Magazine Compass Award winner and selected as Security Magazine's 25 Most Influential People in Security in 2009. George is a graduate of American University; a life member, former president, and Board member of the International Security Management Association; and an alumnus of the US Department of State, Overseas Security Advisory Council.

METERS AND DIALS—TRACKING AND MONITORING KEY RISK INDICATORS

Just as we use the gauges on our car to monitor the status of critical components, security's metrics may be organized to provide a selectable variety of indicators to support our ability to anticipate and avoid hazards and risk. This next discussion provides multiple examples of how we can build and present our information for internal tracking and security program management while also delivering some essential reports to management.

> *Take special note of the critical importance of an established, reliable incident reporting and information management process to developing and communicating on risk. Ensure that any sensitive data receive the level of protection established by policy or as directed by counsel.*

I believe one of the most important objectives of a corporate security organization is to maintain a variety of processes calculated to provide the enterprise with timely, actionable, and reliable information on the full range of security-related threats and risks confronting the enterprise. Key risk indicators are the metrics that enable management to gauge its appetite for risk, measure performance of its safeguards, and address gaps in protection.

KEY RISK INDICATORS AT THE ENTERPRISE LEVEL

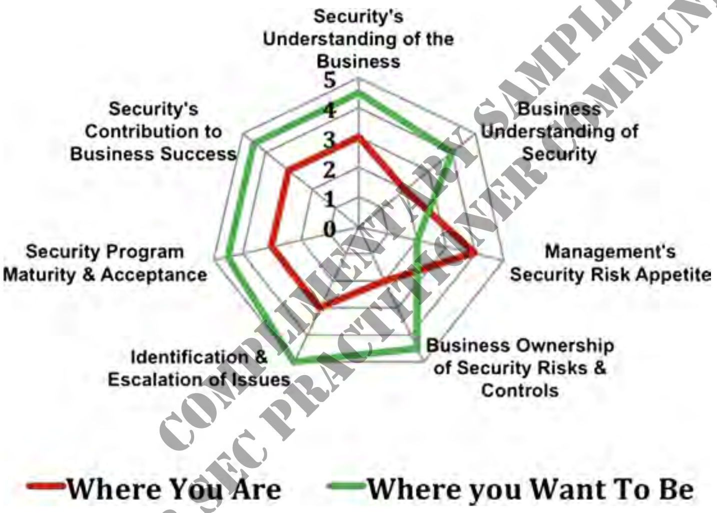
How connected is your security organization to senior management's business and risk management strategies? How connected are they to your programs and their shared responsibilities for enterprise protection? Probing the quality of these connections should be a core element of the security executive's risk management agenda. Consider the following approach to support this probe.

An interesting and often revealing conversation takes place when a security leader sits down with his or her boss or a senior executive from a business unit and asks them to rank on a scale on which 1 = low to 5 = high questions like the following:

- What is management's appetite for security risk?
- What is management's level of knowledge and understanding of the security mission?
- How well do you think we in security understand the business?

- To what extent do you see business units taking ownership for security risk and controls within their areas of operations?
- To what extent does management see security contributing to the success of the business?
- What is your perception of the maturity and acceptance of the security program here?
- Do you believe security risk issues are appropriately identified and escalated from the business units to security?

The quality of our communication and the metrics that accompany and support the messages are key players in influencing and informing management's appetite for risk. What we see in the following chart is a failure to communice at a critical level. There is a fairly significant disconnect between the parties on where the business sees risk and the perception of security management. It appears that the lack of a shared strategy is at the heart of some real problems here. Management's risk appetite is higher than it should be, and the business in not appropriately engaged in ownership of risk controls because it really does not understand what security does or how it can contribute to enterprise success. Nor does management see security effectively understanding the business, so how can they talk the same language? At this point, it is not possible that this security organization can effectively drive security policy, impact risky business practices, or build a collaborative relationship with their key business clients.



This is a conversation that every security executive should have with their business leaders. These are fundamental questions that have answers that not only drive a strategic and measurably effective relationship. They are the essence of enterprise risk management.

SUMMARY

A chart like this provides an excellent opportunity to discuss the relevance and resilience of key business relationships with the security program and the template is easily found in your PowerPoint application. This is an example of how key risk indicators (KRIs) might be illustrated in assessing where you are at a point in time against where your organization's security program aspires to be. I have found this little drill to yield interesting discussions between security managers and their boss or others in senior leadership. The idea is simple: you pick several key risk indicators at the enterprise level and then score where you believe the company lies on a scale on which 1 = low/bad to 5 = high/best. Then get the scores from your top executives. I bet you end up with some interesting differences of opinion from different sources.

The bottom line is that KRIs should be "key" risk indicators—macro level and focused on the enterprise. There are no magic indicators, but there are some (tone, appetite, transparency, ownership of controls, etc.) that line up with what others in audit, legal, risk management, etc. may be conveying. Try this out on a colleague there to refine your selection.

In this example, we are using several indicators that are keyed to reflect how security is seen as an element in the governance infrastructure and to elicit some honest opinions on security's role and level of alignment with the business. How you resolve where you think you are versus where your CEO quantifies these factors is your problem. I guarantee that it is a discussion worth having. Think about how that conversation might go in your organization.

Now, let us take a more detailed look at key risk indicators.

KEY RISK INDICATORS AT THE CSO LEVEL

Does a CSO have a *legal* obligation to inform management about risk? Is there a fiduciary obligation? Ask your legal counsel. This is an important consideration in metrics reporting by members of the corporate governance team.

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 KRIs to their corporate management and, through appropriate gates, to the board.

An excellent research paper commissioned by the Committee of Sponsoring Organizations of the Treadway Commission[7] (COSO) entitled "How Key Risk Indicators can Sharpen Focus on Emerging Risks" summarizes the purpose and value of these metrics as follows:

> *"The development of KRIs can provide relevant and timely information to both the board and senior management, which is significant to effective risk oversight. Effective KRIs can provide value to the organization in a variety of ways. Potential value may be derived from each of the following contributions:*

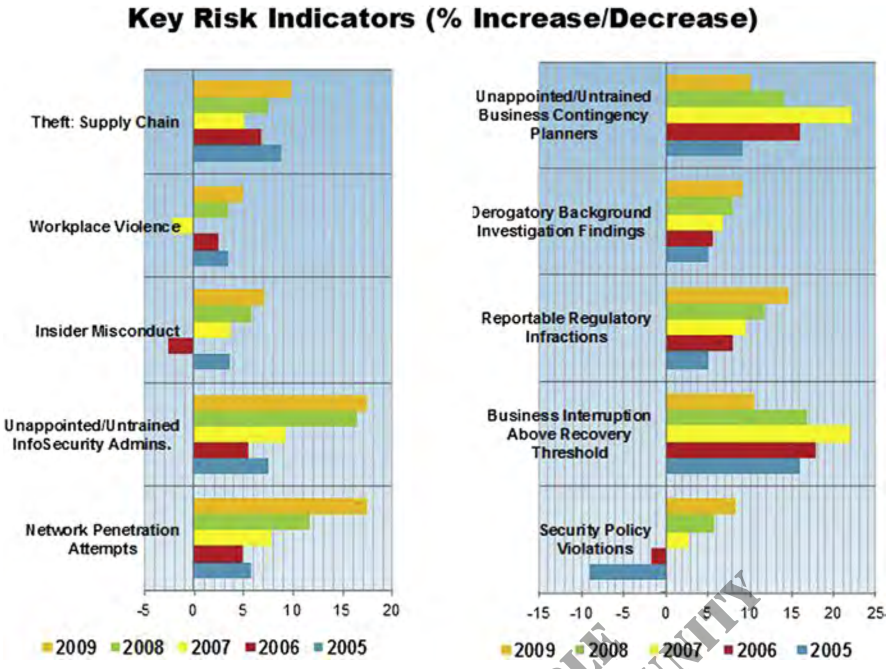
[7] "How Key Risk Indicators can Sharpen Focus on Emerging Risks", Mark S. Beasley, Bruce C. Branson, Bonnie V. Hancock, Committee of Sponsoring Organizations of the Treadway Commission, December 2010.

> ***Risk appetite****—KRIs require the determination of appropriate thresholds for action at different levels within the organization. By mapping KRI measures to identified risk appetite and tolerance levels, KRIs can be a useful tool for better articulating the risk appetite that best represents the organizational mindset.*
>
> ***Risk and opportunity identification****—KRIs can be designed to alert management to trends that may adversely affect the achievement of organizational objectives or may indicate the presence of new opportunities.*
>
> ***Risk treatment****—KRIs can initiate action to mitigate developing risks by serving as triggering mechanisms for organizational units charged with monitoring particular KRIs. As well, KRIs can serve as controls by defining limits to certain actions.*
>
> ***Risk reporting****—By design, KRIs can provide measurable data conducive to aggregation. Summary reports can be quickly communicated to appropriate senior managers and board members with oversight responsibilities.*
>
> ***Compliance efforts****—For organizations subject to regulatory oversight, KRIs may be useful in demonstrating compliance with established requirements.*
>
> *KRIs designed to assist the board and executive management in anticipating trends in potential risk-related events can add considerable value to enterprise-wide risk oversight efforts by positioning the board and management so that they can proactively adjust strategies in advance of or in response to risk events. The design and roll-out of a set of KRIs is an important element of an organization's enterprise risk management process."*

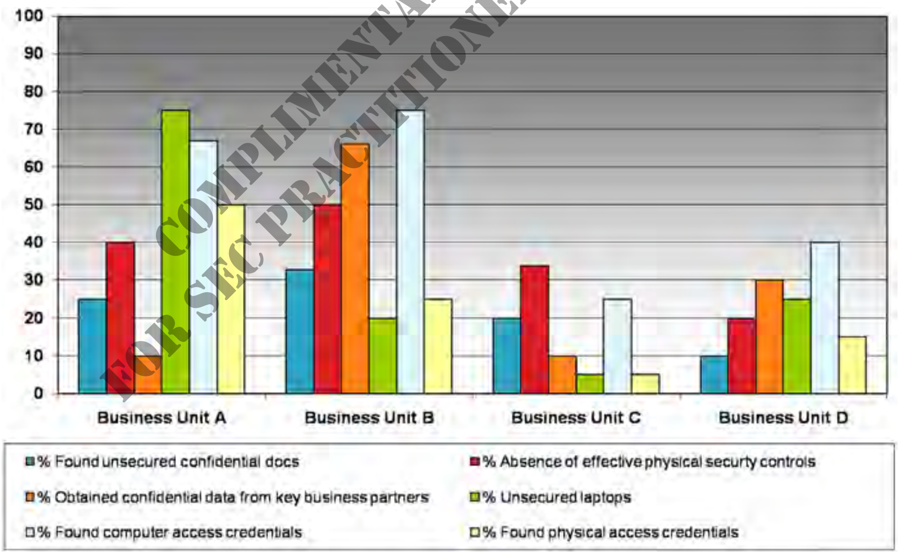
Key risk indicators are your tracking tools for avoidable risk management and security awareness.

I have found that establishing a linkage between key performance indicators (KPIs; discussed later in this book) and KRIs to be a highly effective means of communicating what we know about the root causes of risk and how well accountable parties (including security) are doing in meeting risk reduction objectives. KRIs, after all, impose a defined set of actions.

In the following example, the CSO has selected a variety of KRIs for quarterly management reporting. He might choose to focus on the relationship of a couple of trends like untrained information security administrators and network penetration attempts or regulatory infractions and internal misconduct. There is program performance progress visible here, as well as disturbing leading indicators that have gone ineffectively addressed. This example may better serve as a summary display given the diversity and amount of data presented. What it does offer is a dashboard that provides longer-term trend data to contribute to program performance assessment and focus targeted audiences on areas requiring increased engagement. There are likely linkages between several of the internal risk trends seen here that should be driving analysis and collaborative efforts across the corporate governance team. The correlation of the timing of economic recession on this company is also a potential contributor that deserves probing.



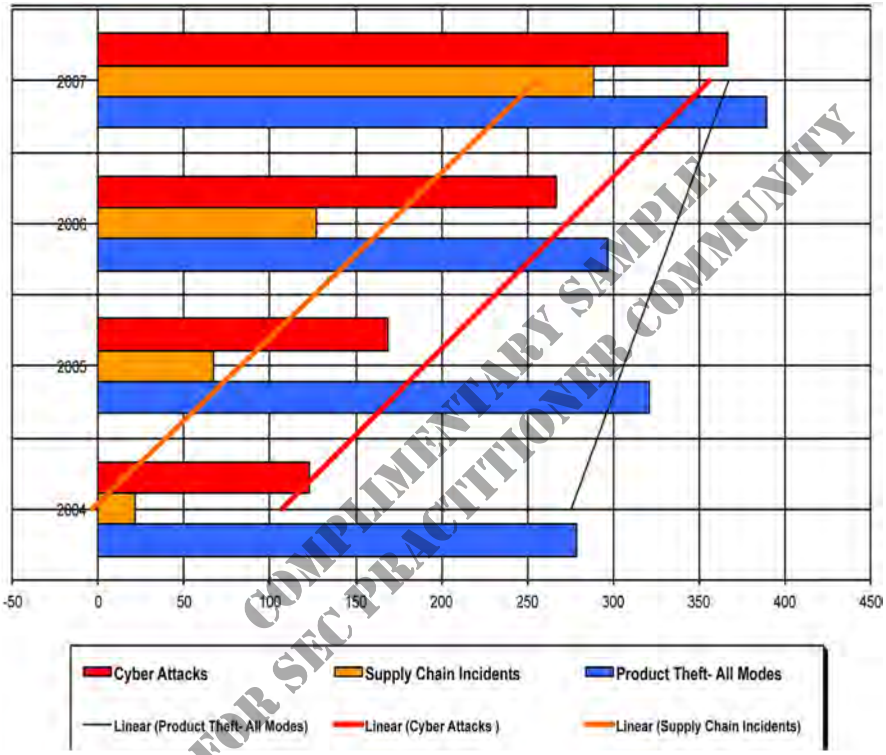
In the graphic below, the CSO is focusing more specifically on four business units, thus enabling a more pointed discussion on the stewardship of local management for basic security responsibilities. Here, KRIs are not being used as a sharp stick in the eye, but should serve to demand far greater accountability.



Remember that KRIs are critical leading indicators that may signal emerging internal or external risks and that our data are often the singular lens to interpret and provide insight to boards and top management. This is particularly true when that lens is effectively focused and aligned with corporate business objectives. This is an example of ability to enable the business to engage in prospective risk management and another key value indicator for security's programs.

TAKE A DEEPER DIVE ON MULTIYEAR TRENDS TO HIGHLIGHT RISK

In the following chart, you can see use of trend lines to focus management on three areas of loss, which obviously deserve more attention. This is where just counting does serve to shine a light on a variety of internal control failures that must be acknowledged, strategized, and mitigated. This is the use of reliable, collated data to eliminate plausible denial and force a discussion on the acceptability of notable categories of risk.

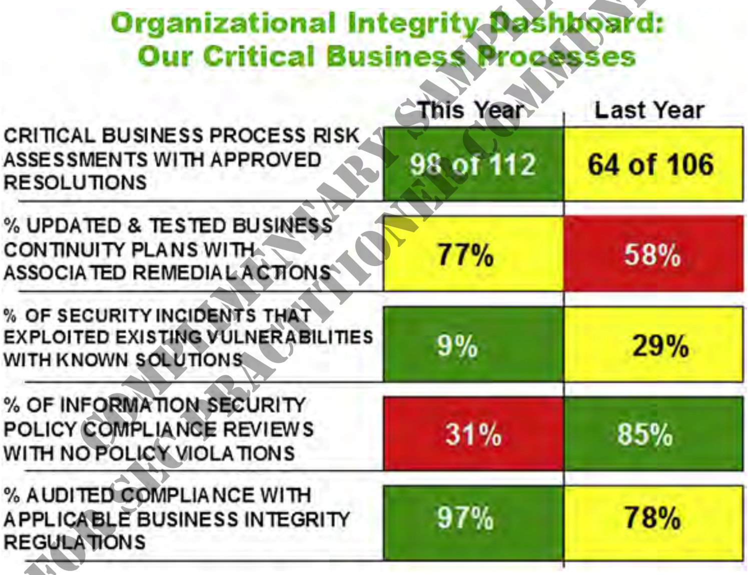


But the real story behind this chart is the absence of attention and accountability. The data have been there, increasingly flying these red flags for four years! One has to wonder where security management was looking and seriously question the condition of the company's risk management program. Cyber attacks are up 188%, and there has been a 56% increase in product thefts and a 13-fold increase in supply chain security incidents. This dramatic supply chain statistic was later found to have its root causes in the total lack of risk assessment and controls associated with extensive outsourcing initiatives in Southeast Asia and Mexico.

Would an established program of tracking and reporting on these areas of business risk have arrested these avoidable losses? Not without access and engagement of management. If you are appropriately investigating and documenting incident findings, having the right data is the easy part. The ability to influence policy and action is the test of security management's use of its information and the metrics that flow from it.

BUILD A RISK INDICATOR DASHBOARD

We need to find responsive ways to display and communicate the key information a manager needs to monitor a set of measures and effectively communicate the status of those measures. You are busy, and so are those you seek to inform. Immediate comprehension of business information is essential. The data in a risk indicator dashboard are presented in such a way as to maximize understanding with a minimum of explanation. You also reinforce basic security policy with periodic updates like this.



Organizational Integrity Dashboard:
Our Critical Business Processes

	This Year	Last Year
CRITICAL BUSINESS PROCESS RISK ASSESSMENTS WITH APPROVED RESOLUTIONS	🟩 98 of 112	🟨 64 of 106
% UPDATED & TESTED BUSINESS CONTINUITY PLANS WITH ASSOCIATED REMEDIAL ACTIONS	🟨 77%	🟥 58%
% OF SECURITY INCIDENTS THAT EXPLOITED EXISTING VULNERABILITIES WITH KNOWN SOLUTIONS	🟩 9%	🟨 29%
% OF INFORMATION SECURITY POLICY COMPLIANCE REVIEWS WITH NO POLICY VIOLATIONS	🟥 31%	🟩 85%
% AUDITED COMPLIANCE WITH APPLICABLE BUSINESS INTEGRITY REGULATIONS	🟩 97%	🟨 78%

RISK MANAGEMENT STRATEGY

With an increased focus on transparency, regulatory compliance and board-level reporting, directors, CEOs, and CFOs have been increasingly open to immediate, proactive, and glaringly obvious warning lights. Your corporate security program can use this type of traffic light image in dashboard dials to present information to management on risk indicators. This next graphic provides a simple set of risk indicators that have been selected for a senior management briefing. The comparative data reflect several business processes the risk management team has selected under the heading of organizational integrity. The significance and tone is set by the fact that the data are based on confirmed results—risk assessments, compliance reviews, and incident postmortems.

It is also clear that this organization maintains an aggressive, ongoing program of risk assessment, the results providing high-level visibility and influence to the security team. If I were briefing this chart, I would be ready for some interesting discussion around the percent of incidents that exploited existing vulnerabilities with known solutions. What five critical business process risks are you tracking and reporting? What are the implications for top management and owners of the business process? What do you propose that security will do, and what are your recommendations for the process owners? How will progress be measured?

MEASURING RISK ASSESSMENT PROGRAM EFFECTIVENESS

It may be said that the absence of an effective risk assessment program should be at the top of the key risk indicator checklist.

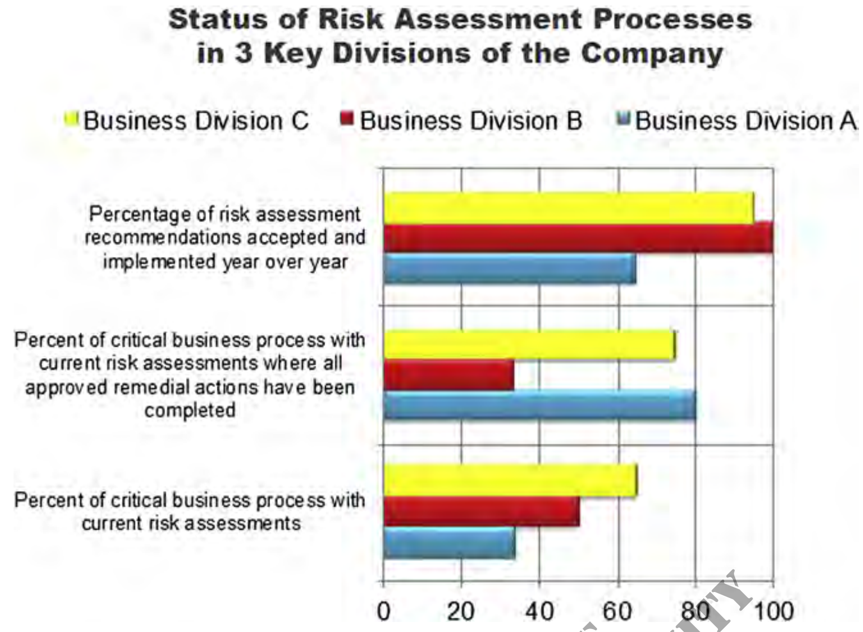
Look at the continuum in the three metrics reported on the chart below. First, we are doing risk assessments; second, the results are driving remedial action; third, security is leveraging its role in enterprise risk management; and fourth, there is a clear trend of business unit engagement. But are we seeing good news or bad in this chart?

Is there is a lack of apparent maturity in this risk assessment program? The advertisement is for “3 key divisions,” all of which clearly possess critical business processes. However, on average only half of these critical processes have been engaged in basic risk assessment.

Look at business division B as an example.

- Half their critical processes have been risk assessed, but which half?
- Of that half, only a third have approved remedial actions. So do we feel satisfied with understanding this level of exposure around only 17% of this unit’s critical processes?
- 100% of our recommendations have been accepted and implemented for this portion of B’s critical processes. Was this acceptance driven by the potential for consequences, influencing by security or something else?

If you were the CEO looking at this chart, what questions would you ask and why? If you were the CSO presenting, what story would you tell if you only had a 5-min slot? Or, as the CSO, how would you have delivered a heads-up alert to the executives of these three divisions that you were going to brief this to the CEO? You are looking for responsive collaboration around change and building bridges. But if they take the wrong turn, you still have the evidence on your side.



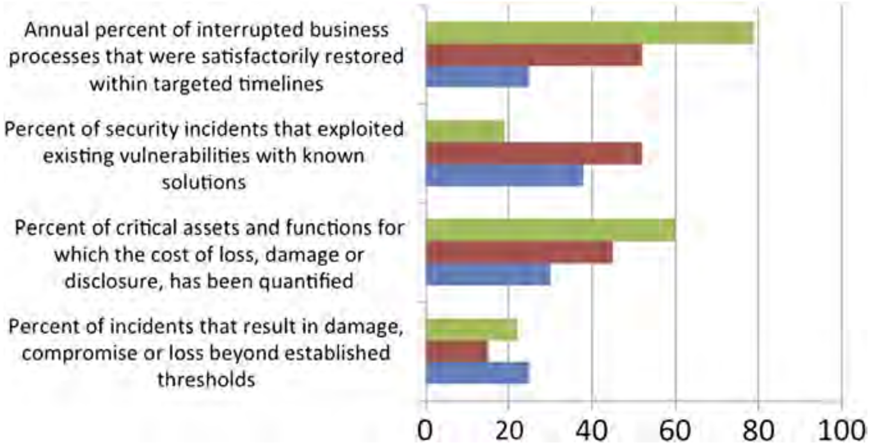
Here is another view of how focusing what we learn from our risk assessments in the right places with the right information can be a powerful incentive for improved risk management.

In this example, we see a security program that has effectively tracked losses and critical process downtime attributable to defective internal controls, pushed deeper and more focused risk assessments and deployed a variety of tools for proactively identifying risky behavior.

Coupling solid risk assessment results with key risk indicators that are supported by root cause analysis offers up headlines that get management attention. Our objective is to eliminate plausible denial. But we have an obligation to probe and inform and targeting those risks that can threaten the franchise provides an incredible opportunity to put the security program positively in front of senior management and the board.

IDENTIFYING THE THRESHOLD OF "ACCEPTABLE" RISK

What is an "acceptable" risk in your world of exposure to security risk management? How much loss can be tolerated before some threshold of damage is breached? We know that zero risk is as unachievable as 100% protection, but without somehow pushing a consensus notion around some baseline target, we cannot get a handle on how much resource to devote to protection activities. Essentially, we are probing the company's tolerance for risk, and this is a critical discussion that too few security managers are prepared to have with senior management.



What factors help define an appropriate level of acceptance or tolerance? Here are a few:

- From our history, it is not probable and below what we can accept as intolerable.
- The consequences of occurrence are reasonably deemed to be minimal and manageable.
- The cost of protection is likely more than what we can estimate for total impact cost.
- Our insurers, regulators, and authorities say it is acceptable.
- The benefits outweigh the potential risks (for example, we will do business in a risky region with significantly lower costs and higher payoff).

The four measures seen in the above chart are linked to the need to identify potential, probable, and known impact from security-related events. But, of importance to a business-centered security manager, each one contributes to considerations around return on security investments, assessment of cost effectiveness, and program performance measurement.

Percent of critical assets for which a cost of loss, damage or disclosure has been quantified

This is absolutely key to protection planning and program management. Our whole risk management scheme relies on the ability to understand, in real economic terms, what the consequences of compromise could be given a set of rational—not absurd—scenarios. This is why linking what is learned from business continuity planning about recovery timing and cost is relevant to security resource management. All security planning should reside on a foundation of delivering the requisite level of protection at the lowest possible cost. “Requisite” means measurably consistent with criticality and consequences of loss.

Percent of incidents that result in damage, compromise, or loss beyond established thresholds

This is a KRI that clearly implies concern for the quality of detective, preventive, and response activities. Here, we have taken the quantified estimate of loss noted above and tracked those incidents that exceed that threshold. Obviously, our goal is to see that no incident has an impact beyond that standard and that can help define protection plans and safeguard capabilities. A simple example is a 5-min standard for response to certain types of calls or alarms.

Annual percent of interrupted business processes that were restored within targeted timelines

This is the counterpoint to the one immediately above, at least as it applies to business continuity risk. But you could extend to "percent of theft incidents with acceptable levels of recovery" or "investigations completed within planned cost" or any number of similar measures. These are important key performance indicators.

Percent of security incidents that exploited existing vulnerabilities with known solutions

I hope and trust that you are doing risk assessments. This should be a compulsory metric in every security presentation because it tells a number of compelling stories about security's proactive diligence and business unit accountability.

If you are not tracking metrics like these, I would recommend that you have a discussion with your corporate risk management or finance team. They can advise on how they are approaching larger business process risk tolerance considerations and factors they deem appropriate to impact measurement.