SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

SECURITY METRICS

Measuring Performance:

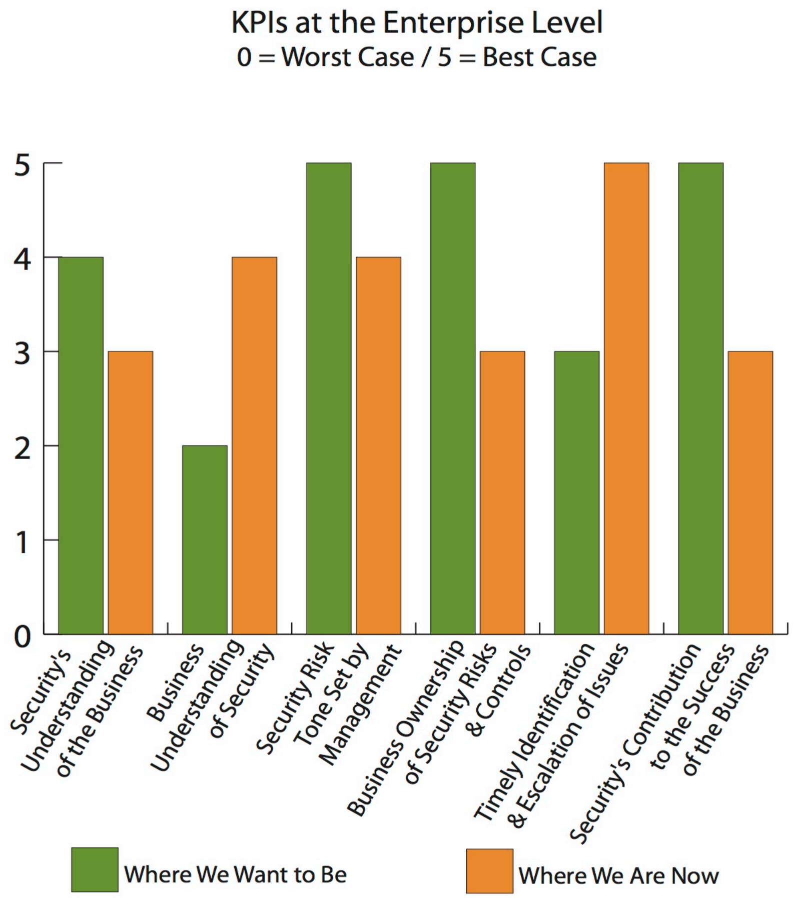
Measuring Key Performance Indicators

Don’t Neglect Key Performance Indicators

Corporate Security Metrics – Key Performance Indicators: Examples

Measuring Key Performance Indicators

By George Campbell, Emeritus Faculty, Security Executive Council



Most of us have heard of Key Performance Indicators (KPI): they are measures of progress toward some goal that often reflect how well a business process is being performed. If you have not considered developing KPIs for your security program, I would encourage you to look at them as a component of your measures and metrics program.

Objective: You have multiple objectives to satisfy your stakeholders and accomplish your longer-term strategy and annual security plan. KPIs provide an effective monitoring tool to measure your progress.

Strategy: In this example, a CSO has selected several high-level directional indicators that are critical to the success of his or her security program (as shown in the graph above). Through a series of interviews with key stakeholders and follow-up security team meetings (injected with a lot of honest introspection), Security has assessed the department's and the business' status (where we are now) against a performance goal (where we should be) on these key indicators. Let me address each of these:

1. Security's Understanding of the Business: This is essential to our ability to understand current and evolving risks and how the business strategy and culture impact our options and approach to security operations and risk management. We gain understanding by engaging with business leaders and thoroughly examining business processes.

2. Business' Understanding of Security: It should be obvious that if the business fails to understand security's mission and value, we will neither be able to influence strategy and policy nor obtain the resources we require for mission accomplishment. Here again, we must be engaged with business processes in activities like proactive risk assessments and incident post mortems and thereby use our unique knowledge to inform and influence. The results of these activities feed our metrics.

3. Security Risk Tone Set by Management: Our success is tied to management's expectations for employee conduct and asset protection. If the business fails to understand how security can contribute to success, it follows that management will set the wrong tone with employees or, worse, will not engage them at all. Explore a variety of venues to ensure awareness.

4. Business Ownership of Security Risks and Controls: Top management should expect business unit leaders to share ownership for effective security practices in collaboration with corporate security. When you use your metrics to inform business unit leaders on protection gaps and problems, you eliminate plausible denial.

5. Timely Identification and Escalation of Issues: When our enterprise security strategy successfully incorporates these prior performance indicators, risk incidents will be identified and escalated in a timely and responsible manner. It will be made clear that avoidance and delay worsen the consequences.

6. Security's Contribution to the Success of the Business: Our status on each of the five preceding desired states clearly impacts our influence and thus our ability to the success of the business. Our status on this final indicator will in part be drawn from our progress on the others.

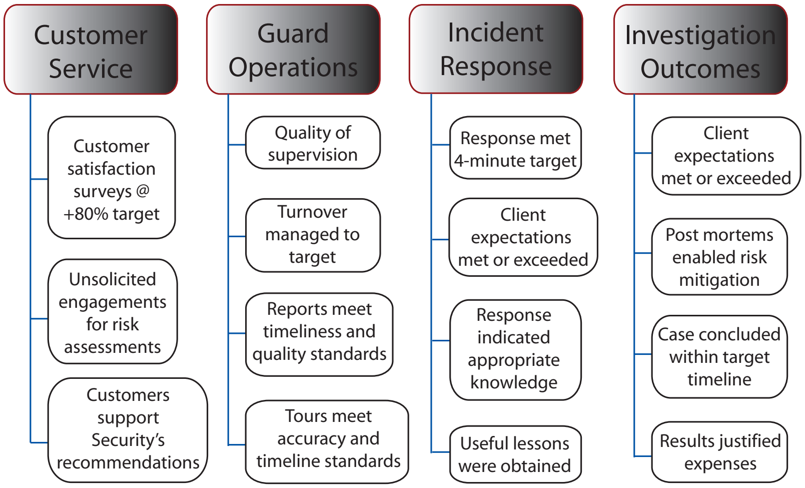
This particular selection of KPIs addresses the question, "What is really important as a measurable contributor to enterprise success?" More quantitative indicators, such as "reduce inventory theft by 25 per- cent by 12/31/2009," are just as valid and actionable and have a proper place in the measurement scheme.

But having a process to periodically con- duct evaluations of these six fundamental indicators anchors the program to a highly qualitative foundation that will pay real dividends to Security's portfolio of value.

Originally Published in Security Technology Executive, May 2009

Don’t Neglect Key Performance Indicators

By George Campbell, Emeritus Faculty, Security Executive Council


Customer Service
Customer satisfaction surveys @ +80% target
Unsolicited engagements for risk assessments
Customers support Security’s recommendations
Guard Operations
Quality of supervision
Turnover managed to target
Reports meet timeliness and quality standards
Tours meet accuracy and timeline standards
Incident Response
Response met 4-minute target
Client expectations met or exceeded
Response indicated appropriate knowledge
Useful lessons were obtained
Investigation Outcomes
Client expectations met or exceeded
Post mortems enabled risk mitigation
Case concluded within target timeline
Results justified expenses

We have mentioned balanced scorecards and KPIs, but it is useful to occasionally revisit these concepts because they can be so much a part of a corporate management business strategy. In our corner of the business, we may employ KPIs in any of several security program areas.

Objective: Organizations use key performance indicators to evaluate their success in reaching long-term organizational goals. We may use them to set specific, measurable objectives for program performance. They may track our success in engaging the business in improved security practices or the progress of vendors in meeting contractual performance specifications. They may set standards for incident response and resolution or any number of desired outcomes tied to the allocation of security resources.

Strategy: In the example above, the security manager has chosen four areas of program performance by which to assess his department’s operations for the year: customer service, guard operations, incident response and investigation outcomes. Under each, the security manager has identified multiple measures he will track to indicate success in that sector of the business plan.

Customer Service. He has set an 80-percent customer satisfaction target that may be measured by post-incident feedback, specific survey exercises or as part of routine one-on-one customer meetings. Additionally, where business units request unsolicited risk assessments and implement a targeted percentage of Security's recommendations, we have clear evidence of solid customer service and alignment with the business.

Guard Operations. Guard force operations typically take up a substantial part of the security department's budget. This security manager contracts with an outside vendor, so he faces issues of liability, co-employment and vendor performance in an industry with frequently high-turnover employment pools. It makes sense to set measurable contractual expectations such as those found in service level agreements (SLA). Our manager has selected four measurable SLA criteria dealing with supervision, turnover and daily competency — each of which contributes to a qualitative picture of vendor performance.

Incident Response. Targeting high-impact performance indicators in this area is a virtual imperative for a security program. Our security manager has set a response time standard that clearly reflects attention to safe and secure workplaces, and he has also identified measures of security team knowledge and customer responsiveness and the highly valued, actionable lessons-learned from incident post-mortems.

Investigation Outcomes. Throughout this landscape of performance indicators, we see our security manager's attention to customer service, here with feedback on client expectations — a potentially sensitive area depending on the implications of investigative findings and results. There is also a continuing focus on management competency, as seen here in the measurement of case duration and cost assessment, as well as the opportunity to contribute to improved risk management through the investigative post-mortem process.

If you are not measuring, you are not managing. We must embed in our minds the imperative of connecting measurable results — critical success factors — with security program objectives. Key risk indicators and key performance indicators need to be the common tools you reach for as you craft the content of your various security programs. They serve to help you navigate the dynamics of risk, better connect and align with the business and its leaders, and effectively manage the often limited resources available to protect the enterprise.

Corporate Security Metrics – Key Performance Indicators: Examples

By Kathleen Kotwica, Ph.D., SVP and Chief Knowledge Strategist; and Greg Kane, Director of IT and Product Technology, Security Executive Council

Many companies have measures like speed, quality and cost to drive value, service performance, and customer satisfaction objectives. To achieve these goals, metrics need to be around the "what" and "how" of measuring program performance.

Key performance indictors (KPI) for physical security are achievable but sometimes security leaders struggle with how to approach this topic – the "how to" dilemma. To get started ask yourself few questions:

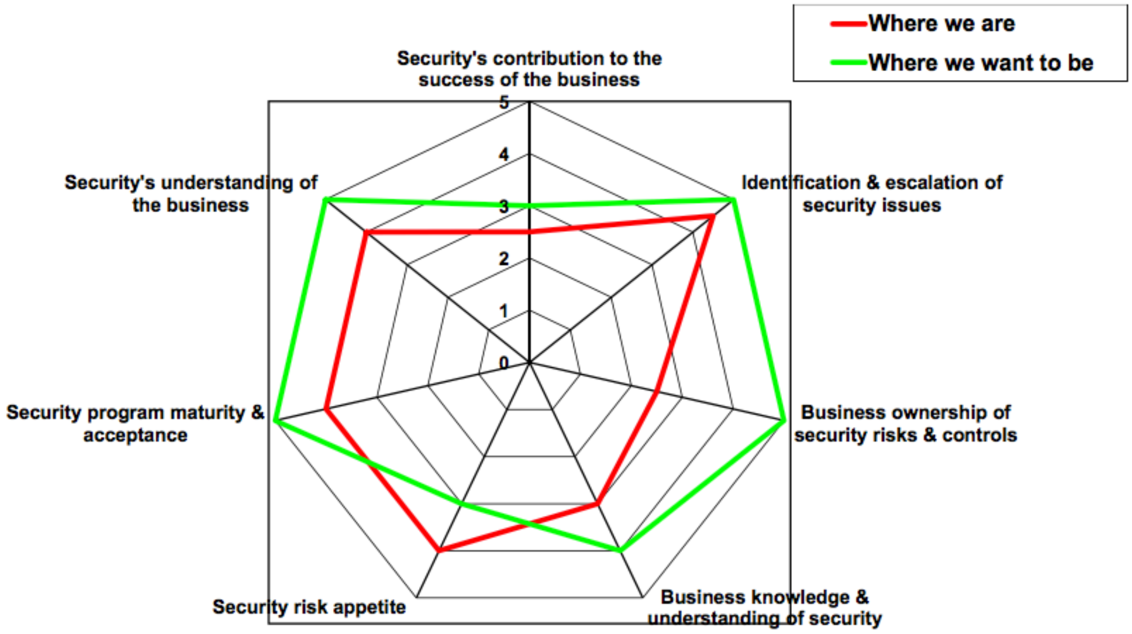
- What are the KPIs that should be driving your team and program's objectives?

- What content is appropriate for which constituents?
- Do you want to influence an outcome or sell an idea or proposal?
- Do you see an opportunity to leverage a collaboration or an improved alignment with a “hard sell” customer?

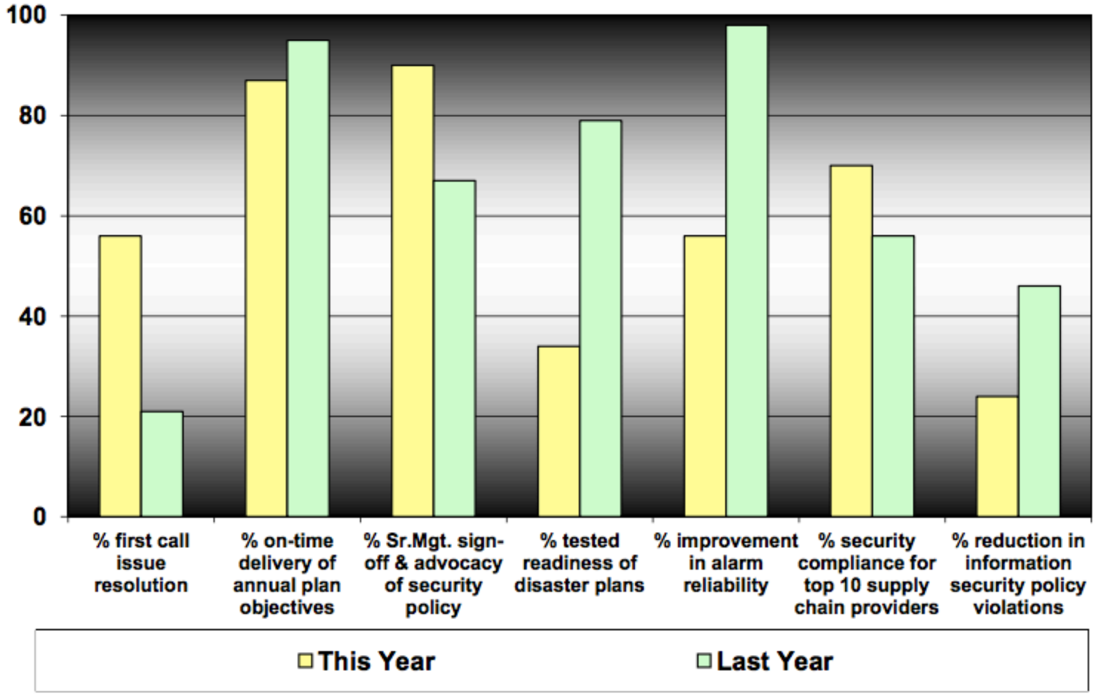
Following are some KPI samples by way of charts that might be used in executive communications. Use them to generate ideas for performance indicators your security organization should deploy.

Originally Published in Security Technology Executive, October 2009

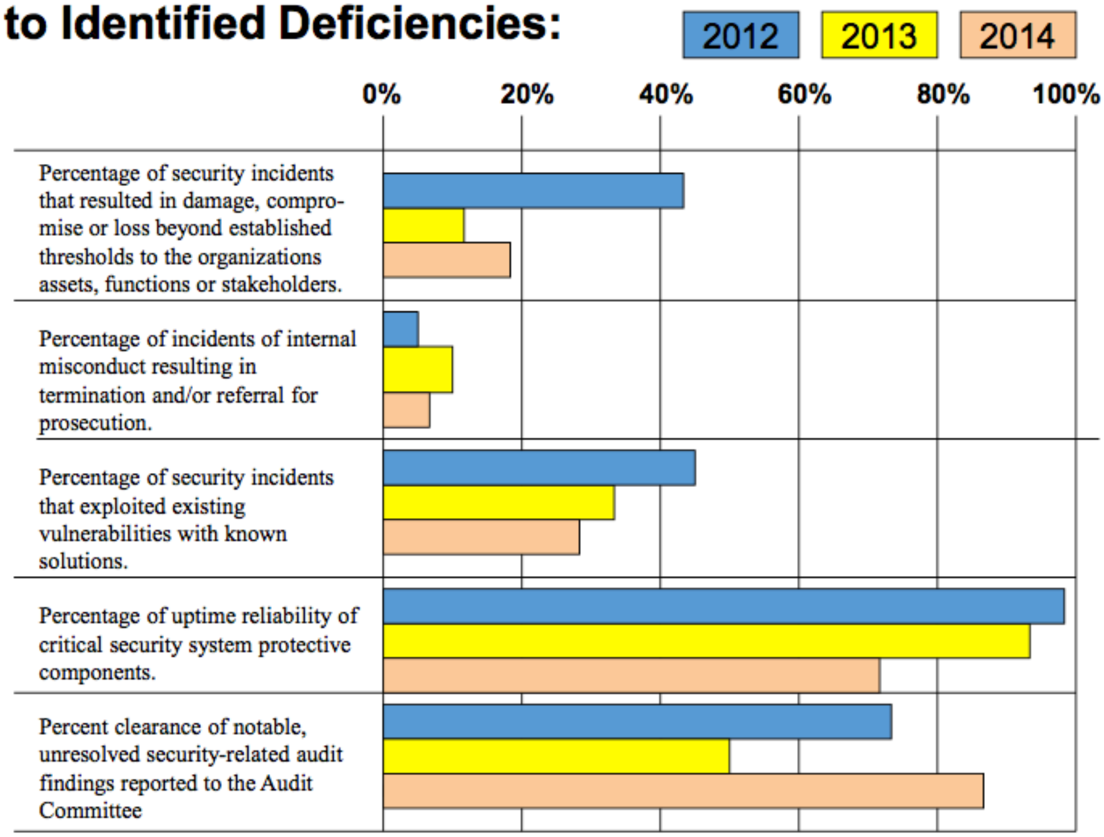
Key Risk Indicators at the Enterprise Level



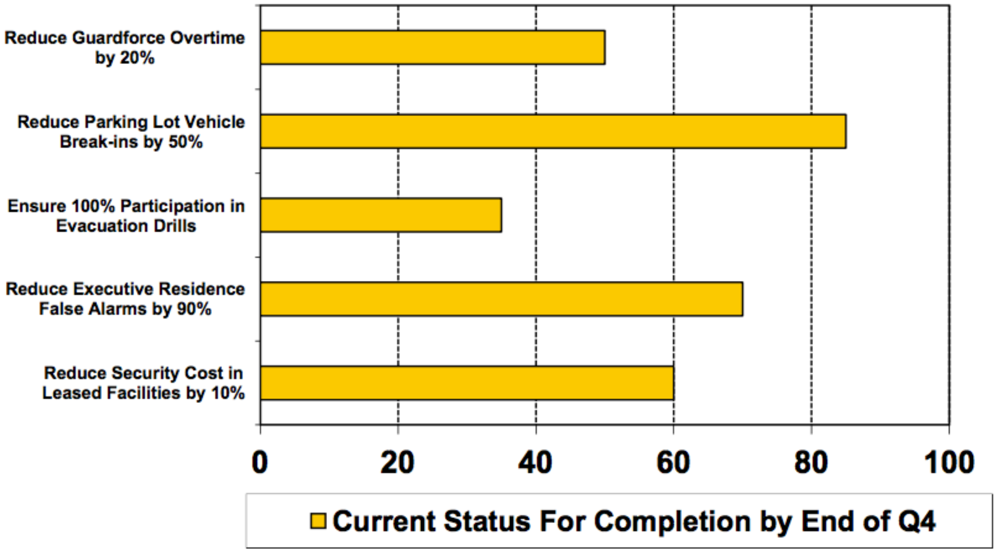
Key Performance Indicators



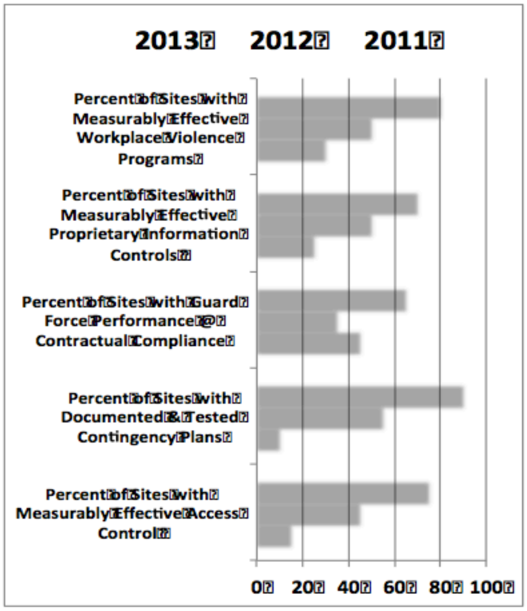
Key indicators of Security Program Response to Identified Deficiencies:



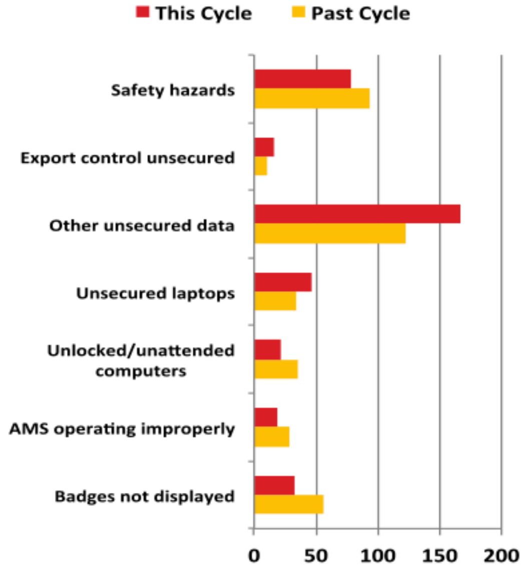
Status of Protective Operations Key Performance Indicators as of Q2



Year-Over-Year Key Risk Indicator Results for Sites Having *Up-to-Date* Risk Assessments

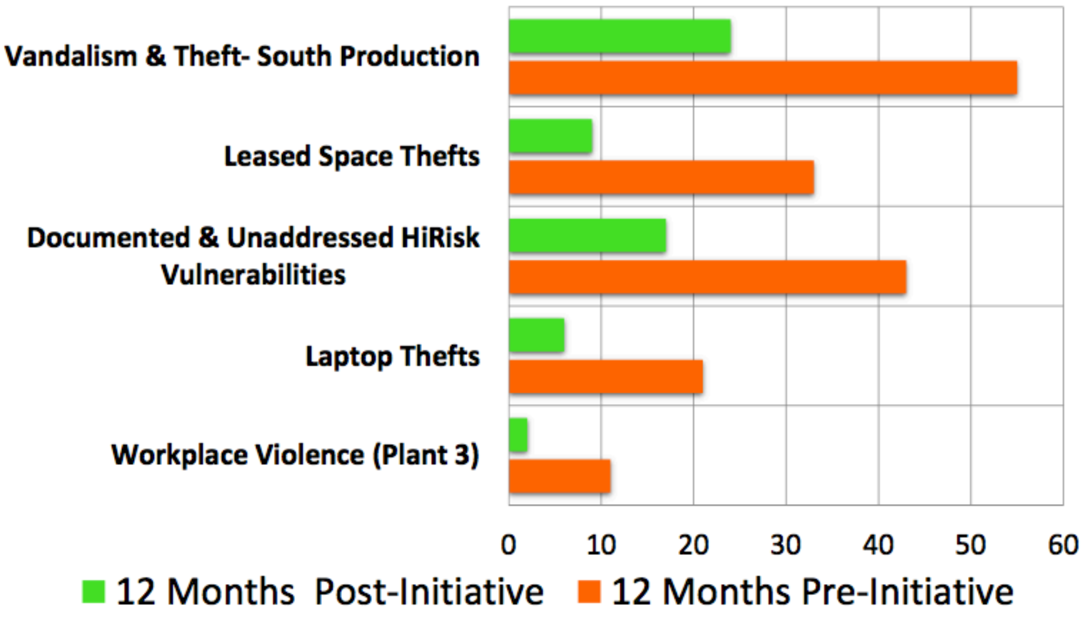


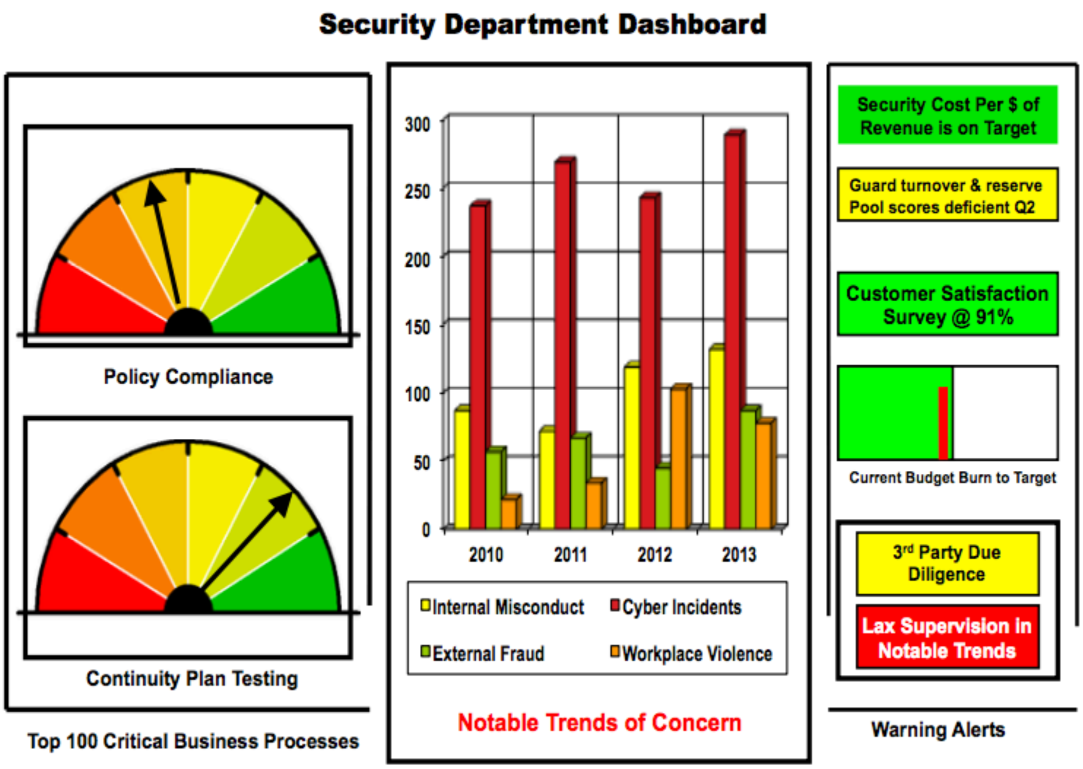
Notable Risk Exposures Mitigated by Inspection Activities & Operational Readiness Reviews



Return on Security Investment (RoSI) = Value:

Reductions in Risk Events Attributable to Defined Security Initiatives





Campbell, author of **Measures and Metrics in Corporate Security, 2nd Edition** and **Measuring and Communicating Security's Value**

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more**.**

Contact us at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com