SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Incident Analysis Identifies Business Practice Risk

George Campbell

Originally Published in Security InfoWatch

October 2008

Incident Analysis Identifies Business Practice Risk

Results: Use this information to inform management of risk trends and to aid in the formulation of targeted preventive strategies. This basic metric will help to ensure management's support of corrective actions and will allow Security to track their effectiveness over an extended period of time.

Risk Management Strategy: In the hypothetical example depicted in the graph, a security department begins using the metric in 2001 to highlight the number of incidents attributable to inside employees. In partnership with Human Resources and Legal, the CSO launches a focused effort to develop, communicate and apply a business conduct policy that leads to a measurable decrease in employee misconduct.

In 2002, the company implements a large-scale contractor program. Consistent use of the metric allows the CSO to identify a subsequent significant increase in inventory losses, systems abuse and customer privacy violations. The solution, which involves more stringent pre-contract security reviews, periodic inspections and procurement oversight, begins in 2004 to measurably reduce the number of incidents attributable to trusted vendors.

Where Is the Data? Effective tracking of data on these three incident types requires much more than Security's investigative reports. Our internal business partners in Human Resources, Procurement, and Audit, as well as various managers overseeing outsourced programs, all have data that represents the more complete picture. Partnering with them gives us solid opportunities to influence policy and strategy.

Significance: This CSO understands the unique risk management perch the security role provides, what metrics are important, and how to track these measurements and use them to successfully engage and influence senior management. The CSO understands that Security is only a piece of the solution and is anxious to collaborate and partner with other members of the corporate governance team.

This metric reflects very significant and sensitive data on the source of threats to the reputation and well being of the company. Knowledgeable insiders are always the most serious threat, since they live inside protective measures. They have a unique understanding of the company's vulnerabilities and know how to use them to advantage.

With outsourcing, we have brought a whole new population into this "trusted" realm: contractors and third-party business partners. You can bet that individual business units don't go around briefing senior management when they have insider misconduct, so it's important that Security maintain the radar. It's the multiple-incident trends, not individual cases, that truly tell the story in this reputational risk area.

What we want to achieve here is change. We need to eliminate plausible denial. Success would be a new or revised policy along with more security-aware business operations that contain the controls essential to safe participation in this new business model.

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, https://www.securityexecutivecouncil.com/secstore/index.php?main_page=product_info&cPath=77_65&products_id=324.*

About the Security Executive Council

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

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