SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Security Metrics > Risk >

Incident Analysis Identifies Business Practice Risk

Created by George Campbell, Security Executive Council Emeritus Faculty

Knowledgeable insiders are a serious threat to an organization since they live inside protective measures. They have a unique understanding of the company's vulnerabilities and know how to use them to their own 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 kind of metrics can we use to track and demonstrate trends in insider misconduct? Let’s consider a hypothetical example.

A security department begins to measure and track 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.

One year later, the company implements a large-scale contractor program. Consistent use of the insider misconduct 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 two years later to measurably reduce the number of incidents attributable to trusted vendors.

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.

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.

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. The information in this article is copyrighted by the Security Executive Council and reprinted with permission. All rights reserved.*

Originally published in Security Technology Executive

Visit the Security Executive Council website for other resources on the Security Metrics: Risk series.

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
Website here: https://www.securityexecutivecouncil.com/

