SECURITY EXECUTIVE COUNCIL
A research and advisory firm

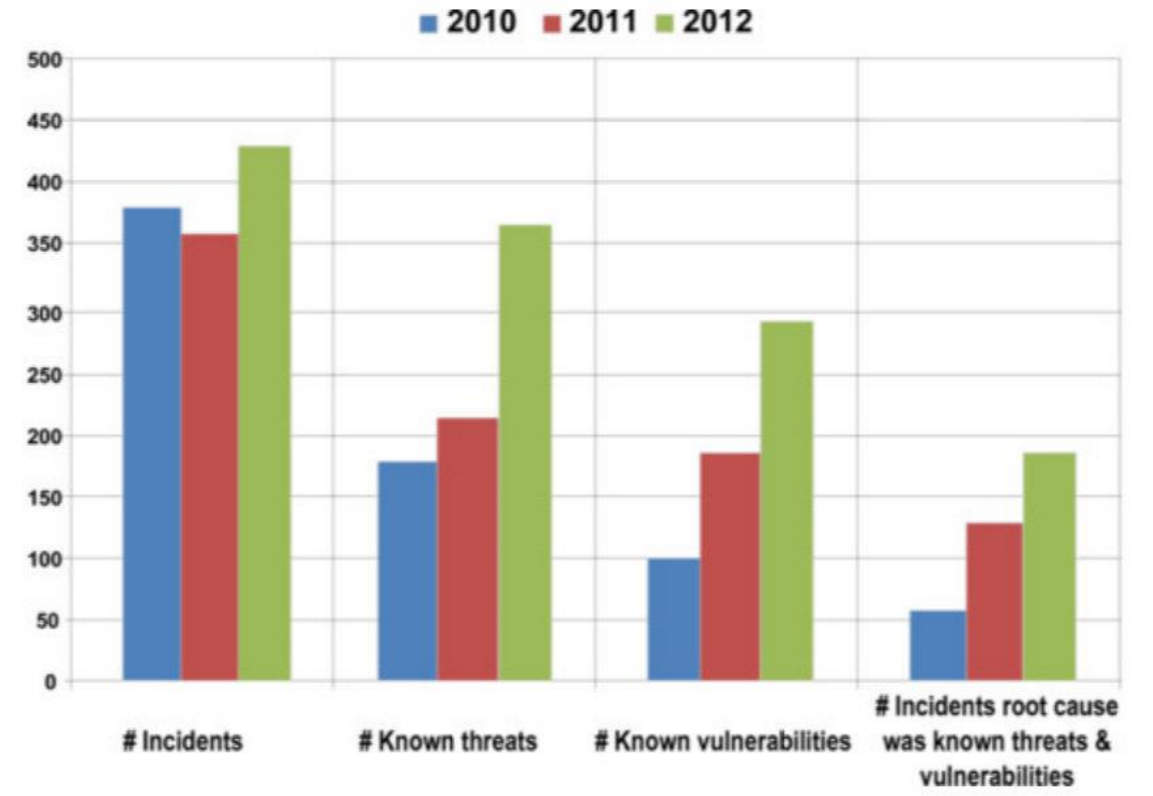
Security Metrics > Specific Examples >

Be a Learning Organization

Created by George Campbell, Security Executive Council Emeritus Faculty

Do you routinely dig into your incidents to identify the root causes and pass on the learning to those who need to know? If not, plan on logging more of the same and documenting allegedly smart people repeating their mistakes — or worse.

Root cause analysis (RCA) is an established process in quality management, engineering and risk management. It may take other forms in our business such as lessons learned, incident post mortems and after action reviews (AAR), but the objectives are the same: to objectively, relentlessly identify the factors that created a failure of a control or set of controls so that those conditions may be prevented in the future. This is about nailing the real cause, not the assumed symptom. Communication is the critical step to record the process and close the accountability loop.



In the example above, we see a corporate security organization that has formalized a process (or combination of analytical processes) focusing on continuous improvement in security risk management. Their approach seeks to understand the degree to which known threats and vulnerabilities are a factor in this company's security incident experience.

What makes this summary analysis particularly relevant is that so many of the protection defects implied here are repetitive. Moreover, from a perspective of consequential risk, these may be events that contribute to personal injury, litigation for defective security, embarrassment to brand, and likely Board inquiries.

RCA is focused on identifying what factors verifiably contributed to the magnitude, timing and location of a risk incident. It forces a broad consideration of multiple sources of incident causation. A variety of human, physical, technical or other factors may contribute to the exploitability of asset vulnerability. What are they? If accidental, what conditions led to the breach? If man-made, how does it appear they were discovered and exploited by the adversary?

Success in this process means changed behavior, tested elimination of process defects, increased awareness of individual accountability, and eventual reduction or elimination of recurrence of like events. Where there may be multiple causes, RCA helps identify a single solution that closes down more than one exposure or isolates a simple, low-cost

approach.

Leverage the learning. I have often heard a colleague say, “What we need around here, every once in a while, is a well-managed incident that grabs management’s attention.” The emphasis is obviously on the “well-managed,” but the notion is sound. Risk is inevitable and the degree to which we are prepared typically tells the tale of the degree of consequence. Engaging a team from the affected business unit, Security and others in corporate governance speaks more to avoiding future risk than taking prisoners. Success can be celebrated and best practices identified or we can learn together what could have been done better.

Companies that fail to learn from their mistakes are destined to repeat them. Be a leader and set the stage for learning.

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 & Design

Visit the Security Executive Council website for other resources on the Security Metrics: Specific Examples 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/

