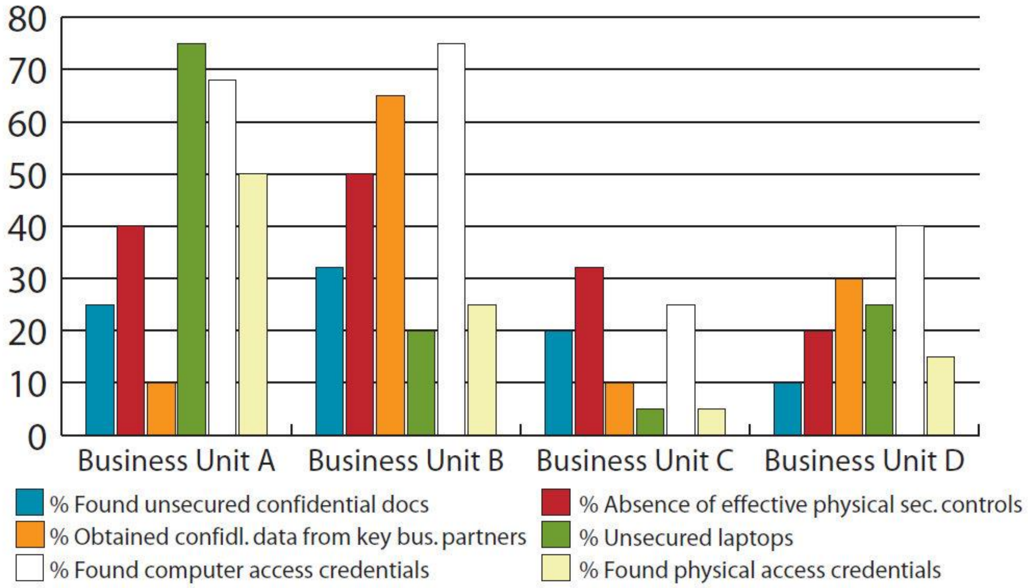
Security Metrics > Risk >

Increase Influence and Protection through Proactive Risk Assessments

Created by George Campbell, Security Executive Council Emeritus Faculty

We security professionals cannot sit back and wait for an incident to happen. We are paid to anticipate risk and engage in preventative activities that will eliminate hazards or minimize the impact on business operations and employee safety.

Our intent with this month's metric is to modify risky behavior within selected business units based on data that has been gathered through security inspections. We seek to encourage the selected business unit leaders to accept responsibility for asset protection.



In the example from which the above graph was drawn, the CSO selected four business units to examine. The selections were based on three qualifying factors:

1. These units provide core business operations, so consequences of loss could have significant impact;

2. A review of incident metrics and security officer patrol logs indicated a variety of potential vulnerabilities; and

3. Security believed it could effectively influence each unit's management to address any shortcomings in security oversight.

The CSO selected security team leaders on all shifts, and at a planning session they reviewed the existing data to target-specific concerns. The teams concluded unanimously that the most potentially impactful security gaps were associated with the protection of proprietary information. Teams then conducted a test run on each shift at each location to further refine the focus of the inspection routines. Security did not advise the business leaders that these inspections were to take place. Anticipating that business leaders may claim that the results were invalid because security has special access, the teams agreed to limit discoveries to those that could be made by any individual having authorized or unauthorized access to the spaces. After defining these parameters, Security conducted 25 inspections at each of the four business units.

The results are seen in the above chart. Business Units A and B obviously have the greatest exposure to risk of information compromise. At Business Unit B, the teams found unsecured confidential documents in 33 percent of the inspections and ineffective access controls (propped doors, unattended visitor entrances, inactive card readers, etc.) in half the inspections. They were able to discover computer access devices or passwords and to obtain confidential data from multiple outsourced business partners in 75 percent of inspections. The undisputed star for unsecured laptops and physical access credentials was Business Unit A. Business Unit C clearly had the fewest discoveries but still has some issues to resolve for proper assurance.

The CSO informed the senior executive of each business unit that inspections had been conducted, and the assigned team leader individually briefed the results. An action plan was developed for each finding as an outcome of these meetings. All findings were turned over to Internal Audit for future review. Because these results presented serious implications for brand protection, the senior management team requested that Security deliver more specific and frequent security awareness briefings to employees.

An unexpected benefit of these exercises: The security officers who were assigned the inspection and follow-up tasks collectively expressed a desire to continue the practice in all facilities on a larger scale of potential risks, and they noted that these activities made them feel like this was truly meaningful work and they were delivering tangible value to the company's risk management program.

Proactive risk assessments like these are low-hanging fruit that delivers real value to the bottom line. They help us avoid potential losses and, given the implications of compromise of highly confidential information, they also measurably improve protection of the company's reputation. But old habits often refuse to die, so a continuing program of proactive risk inspection should be a routine part of security operations.

George Campbell is emeritus faculty of the Security Executive Council (SEC) 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/