SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Risk-Based Security > Risk Assessment >

Transitioning from Risk Assessment to Plan

By the Security Executive Council

Conducting a security risk assessment is an essential first step in developing successful security programs. But what should the security practitioner do with the results?

A brief aside here: The SEC has found that many security leaders are not in fact conducting security risk assessments, and many of those who do are assessing risk only at the site or building level, not at the enterprise level. If you're one of these, stop here and jump over to our page of risk assessment resources, which includes templates, essential considerations, and strategy. If you'd like more on the basics of conducting a risk assessment, a quick web search will reveal a number of other organizations that share their knowledge, such as this page from ready.gov.

If, on the other hand, you have already conducted an enterprise security risk assessment, but you aren't sure what steps you need to take to translate its findings into control measures, this article is for you.

Part of risk assessment is determining whether the organization will accept, transfer, avoid, or control each identified risk. The purpose here is to help the security practitioner move forward in managing risks on the "control" list. To that end, what follows is a brief checklist of action items that can move you from assessment result to program rollout.

- ☐ Identify the source of the risk so that control actions can be appropriately targeted.
- ☐ List business units that would be impacted directly and indirectly by a negative event related to this risk.
- ☐ Measure, if possible, the consequences of related risk events that have occurred at this organization or similar organizations in the past, and be prepared to present this information as part of a business case.
- ☐ If you haven't already, meet with executive management to:
    - ○ determine the organization's risk appetite;

    - explain that executives are the risk owners and must be part of the decision-making process;
    - clarify that there will be residual risk; no control will be 100% effective.
- □ Meet with executive management and the heads of affected business units to:
    - clarify the nature of the risk as it pertains to each unit specifically;
    - find out what they are willing to spend to help mitigate this risk.
- □ Outline your control options and their projected level of effectiveness in controlling the threat. Make sure to consider options based on:
    - Technology
    - Process
    - Policy
- □ Determine and quantify the operational impact of each option in terms of
    - Resources
        - Where can existing resources be leveraged or transferred to lessen the impact of this control option?
        - Where can partnership with other internal units provide access to resources that can be shared?
        - What new resources must be acquired, and what is the projected cost?
    - Staffing
        - Can existing staffing be shifted to adequately manage this control option?
        - What increase in staffing is required, and what is the projected cost?
    - Training
        - How many employees will need to be trained to manage this control measure? Include also non-security employees who will play a role.
        - How much time will it take and what will the financial and productivity impact be?
        - Don't neglect to consider organization-wide awareness training.
- □ Define the roles non-security personnel and leadership will need to play in order to make each control option successful.
- □ Return to business unit leaders and executive management with your identified control options, projected or ballpark costs, and a clear sense of roles. Remember that they are the risk owners; this decision should not be made in isolation. If your organization has an operational risk council, they should weigh in. (An operational risk leadership advisory council is a committee of individuals overseeing the operational level of security risk, which reports to the executive risk management body. For more on operational risk advisory councils, click here.)
- □ Plan how you will communicate the chosen control option. Map your communication choices to the audience and the risk. (For example, kidnap prevention and response plans should only be communicated to executives, while email security measures should be shared organization-wide.)

□ Develop a set of metrics and data gathering guidelines to measure and monitor the effectiveness of the control over time.

Visit the Security Executive Council web site to view more resources in the Risk-Based Security: Risk Assessment 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: https://www.securityexecutivecouncil.com/