Security Metrics > Risk >

Threat Assessment: Measuring Likelihood

Created by George Campbell, Security Executive Council Emeritus Faculty

When you think about security threats to your business, which do you think are likely to manifest? What are the probabilities of a specific type of event occurring at a particular location? How do you convey your concerns to management without sounding like Chicken Little yelling that the sky is falling? It is essential that we keep our eye on "what if." In the security mission, we operate the radar. We possess unique knowledge and perspective on business risk. We have a responsibility to view the risk landscape and scope out the trends, the behaviors and the gaps in common-sense protection and then select the targets and style of our alerts.

Risk assessment clearly involves a threat assessment component, and event likelihood is a critical element. We may view likelihood in a variety of analytical ways, but I like to look at it as the degree to which our exposure to various risks is managed by the strength and effectiveness of our internal controls and security measures. There are scores of measures that might be employed, depending on your company's business risk environment and the scope of its security program, but here are a few to consider.

• The degree to which management supports the establishment and communication of policy and expectations on conduct and security-related responsibilities:

o Security issues are required items on Board agendas.

o Management requires business units to acknowledge ownership of security measures.

o Business conduct policy is in place and supported by action.

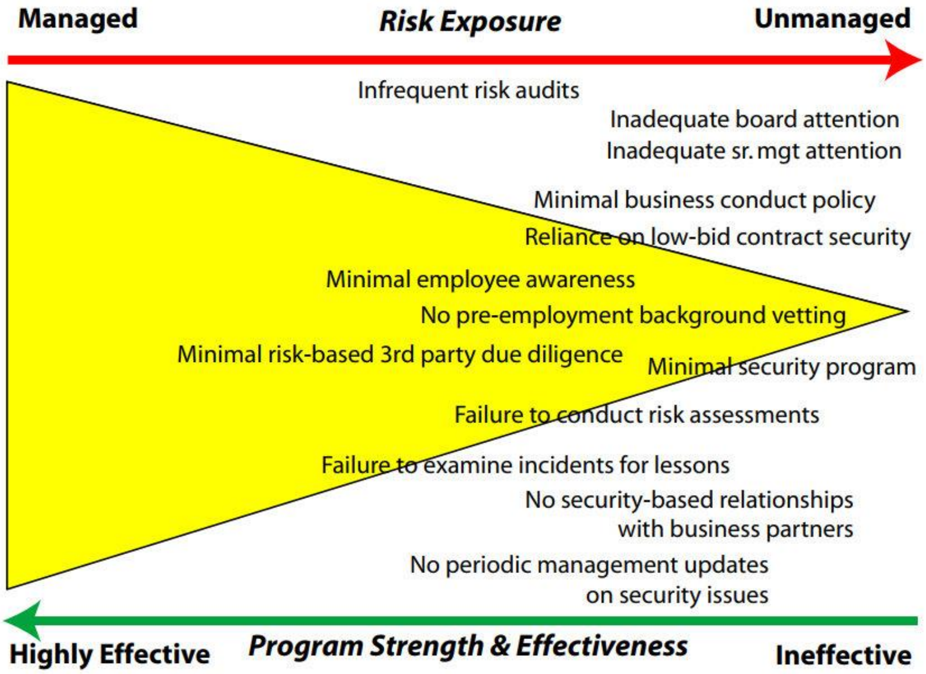
o Background investigation standards are in place and followed in the hiring process.

o Security is regularly on senior management's agenda and takes ownership for supporting corrective actions as required.

    - Management demands timely identification and escalation of issues.

- The degree to which we elect to probe security measure effectiveness:
    - There is a routine for focused risk assessments and internal control audits.
    - There is a routine for tests of security plans and required follow-up actions.
    - There is a routine for targeted incident post mortems and lessons-learned exercises.
    - Employees' awareness of their role in protection is periodically reinforced.
    - Outsourced partners with access to critical business processes or assets are vetted for their commitment to the protection of our brand.

- The degree to which security resources are maintained at a high degree of competency and responsiveness:
    - The security program is clearly established as an element of the corporate risk management infrastructure.
    - Security responsibilities are clearly articulated and personnel are held to high standards of performance.
    - Security objectives are clearly linked to a risk management strategy and plan.
    - Contractors are selected and evaluated on standards of performance rather than just low bid.


Managed
Risk Exposure
Unmanaged
Infrequent risk audits
Inadequate board attention
Inadequate sr. mgt attention
Minimal business conduct policy
Reliance on low-bid contract security
Minimal employee awareness
No pre-employment background vetting
Minimal risk-based 3rd party due diligence
Minimal security program
Failure to conduct risk assessments
Failure to examine incidents for lessons
No security-based relationships with business partners
No periodic management updates on security issues
Highly Effective
Program Strength & Effectiveness
Ineffective

You can construct this list in any number of ways to be consistent with the scope of your security program(s). My list here tends to accentuate the positive, but you could easily list your assessment of the apparent gaps and program shortcomings, as does the figure above. This picture engages senior management's attention, and its serious tone demands a level of verifiable audit and risk assessment findings.

We know that likelihood of risk is influenced by the weakness or absence of safeguards. We need to tell stories to management that eliminate plausible denial, establish accountability, and influence policy and action. A presentation like this connects the dots by showing how the combination of control weaknesses demonstrates an increased potential for business and reputational risk.

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/