

RiskView® Enterprise Management for IT

Why Risk Optimization?

IT risk spend continues to grow, driven by a combination of perception and compliance. Activity is a reaction to tactical "discoveries" and FUD rather than managing one's total security profile against capital spend. The result is often mis-investment; dollars are spent on tools that have little material effect while coverage is thin where it is most needed.

A holistic approach changes the model by stepping back from individual vulnerabilities and focuses instead on portfolio managing material, undesirable outcomes. It seeks to answer three questions:

- 1 – What is my total exposure to an undesirable outcome (i.e. leaking proprietary information)?
- 2 – What should it be against benchmarks, trends, etc.?
- 3 – Where should I increase security investments and where should I decrease investment to reduce my exposure and reduce/optimize spend?

A Risk Management System

Many companies have silos of vulnerability data, spanning tools and processes enterprise-wide. Audit findings may be in one database, compliance survey results in a spreadsheet, automated scan results in an appliance, third-party penetration tests in emailed presentations, configuration compliance records of nonstandard systems in a CMDB, and behavioral analysis engines in their own data store. Ad-hoc processes and dashboards form around these silos to make decisions regarding programs to mitigate each one.

What's lacking is a way to bring this data into a repeatable, scalable framework that looks across the silos, consistently applies best-practices in evaluating the relative risks, and presents business-centric results through an interactive dashboard. In short, an Enterprise Risk Management (ERM) framework and platform is lacking.

With such an ERM in place, a company can identify the total level of material risk of business-impacting events. If the aggregate level in any category exceeds the business's risk-tolerance, materiality filters can be applied to isolate the critical drivers of that risk; controlling those will yield the greatest return on spend. "What-if" analysis can show the effect of such controls in the context of all other risks, and the effects can be profiled and trended over time.

How?

Vulnerabilities have three components: Susceptibility, Exploitability, and Impact. A vulnerability's materiality is represented by the intersection of these: The goal of a Risk

Management Dashboard is to provide actionable information regarding areas of material residual risk. It does this by classifying vulnerabilities into portfolios of undesirable outcomes, and scores both typical and total risk for each class. It then presents residual risk so as to "light up" areas where risk is overly high (requiring investment) or low (less investment required). It provides metrics which can be used as benchmarks, and which can be trended over time.

Rev2's RiskView approach uses a novel, patent-pending interface combining spider graphs and pie charts with histogram-based filters and metrics, materiality-scored based on CVSS (Common Vulnerability Scoring System) standards. Once identified, investments in controls can be redirected to areas most in need. Filtering, sorting, and drill-down capabilities allow for rapid identification of common controls, yielding high return on capital spend. Note that controls can effectively mitigate any vulnerability component (i.e., become less susceptible, make the vulnerability environment less exploitable, or reduce the impact).

A number of internal and external sources of data may be leveraged, so long as vulnerabilities are classified and scored consistently (the portfolio approach tends to reduce errors in the system as they cancel each other out over large data sets). Sources of vulnerability data can include self-assessments, audits, SIMISEM, behavioral analysis, application-infrastructure mapping tools, and configuration vulnerability analysis. Optional external sources might add NVD (National Vulnerability Database), FIRST, SANS, CERT, CAIDA, IT-ISAC, etc.

Summary

An Enterprise Risk Management tool, applied to IT Risk, can focus resources by providing visibility into where material residual risk exists and where it does not. It provides actionable feedback as to where the greatest needs for controls are, what risks are materially driving that need, and where additional controls will add little value. This is achievable through a combination of scoring, visualization, and benchmarking. RiskView provides these capabilities in an extensible, scalable platform.

Contact us today for a Proof of Concept tailored to your business: info@rev2.com, 914.614.8600.

Copyright © 2011, Rev2. All rights reserved. The RiskView® application is a registered trademark of Rev2. All other trademarks in this document are the properties of their respective owners.