

Application of Risk Management Principles in Information Technology Permitting Decision Makers to Target Funding for Security Investments

by Dr. Martin A. Carmichael, Chief Information Officer, The Rader Network,
Colorado Springs, Colorado

Abstract

Federal, state, and corporate security officials find it difficult to communicate with decision makers – in the business terms they understand – why investing in information technology security is an imperative¹. In particular, Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) must effectively explain that security is not an overhead cost but a business enabler, allowing organizations to comply with the Sarbanes-Oxley Act and other governance regulations. This is largely due to the fact there has not been a cost effective, efficient, or comprehensive tool to establish a mathematically-provable business case. Statistical analysis software that applies risk management principles to information technology has been developed to resolve this inadequacy. Technology Risk Manager (TRM) software is specifically designed as a comprehensive strategy to meet the challenge of creating defensible, cyber security business cases.

Problem

The combination of increased vulnerability, increased stakes, and increased threats make cyber security one of the most important emerging challenges in the evolution of modern cyber infrastructure design and deployment.² Correspondingly, there is increased difficulty to establish a “return-on-investment” business case that decision makers can understand and appreciate as cyber infrastructures become larger, more complex, and more distributed. Security officials must be able to communicate the importance of information technology security in terms easily understood by those who control investment in cyber infrastructure design and deployment to prevent loss of life ... and the loss of our way of life.

“If you can’t measure it, you can’t manage it.”³ Regardless, organizations develop budgets and expend funds without an effective means of measuring information technology security. For example, Gartner Incorporated advises organizations to spend from 4% to 6% of their information technology budgets on information security. Yet determining “bang for the buck” is currently subjective, indefinite, ad hoc, indefensible, and lacking in scientific methodology.

Information security budgets are expected to increase 4.5 percent in the next year.⁴ As with the Maginot Line, it is becoming increasingly difficult to build affordable information technology protection defenses.⁵ Organizations that can accurately measure information technology risk can reduce costs.

Approach

Not all numbers qualify as metrics. The so-called “metrics” currently captured during network scans are simply counts -- patches to upload, vulnerabilities noted, past security compromises, etc. The metrics that result from TRM analyses are true metrics that can be scientifically scrutinized. TRM metrics are numerical facts based on statistical analyses. TRM metrics are objective, quantitative, repeatable, and defensible. TRM metrics predict the likelihood of security failure within an information technology environment along each of the four dimensions of risk: confidentiality, integrity, availability, and audit. TRM Risk Indices describe the likelihood of security failure as a statistically-derived percentage along each risk dimension within a defined period of time and a baseline threat. Each process on an enterprise is evaluated for its security characteristics. Adjacencies are measured and the results are aggregated to determine each host’s security characteristics. Adjacencies are measured a second time and the host calculations are aggregated to calculate the Risk Indices. TRM provides a systemic view of information technology security, empowering managers to direct this activity with the same precision they use to manage risks in their other resources. Upon establishing a baseline, a TRM-certified user can accurately model and simulate how strategies and technologies can be best used to protect assets. Decisions can then be made based on proactive analyses and predictive modeling. TRM reduces the certification and accreditation reporting process from months to weeks. TRM converts information assurance from a subjective to an objective management process.

Results

We can only trust what can be quantitatively measured. Implementation of the modeled and simulated recommendations following a TRM analysis historically have resulted in an average 19% decrease in overall risk within an enterprise.

Conclusion

TRM is commercially available software specifically designed to empower security officials to determine return on investment in objective, quantitative, repeatable, defensible, and predictive terms. The selective outputs of a TRM analysis yield results that can be certified and accredited versus in hypothesized prose. TRM provides quantitative metrics of information technology security, which enable users to specify security requirements, formulate security claims, and certify security properties as a comprehensive strategy to meet the challenge of creating defensible, cyber security business cases. TRM is specifically designed as a comprehensive strategy to meet the challenge of cyber security in the 21st century. TRM permits information technology security professionals to shift their focus away from winning battles towards the strategies to win the war. TRM will elevate trust in critical infrastructures. The Rader Network sincerely believes that TRM will fundamentally change information technology security as we currently know it.



Bibliography:

- ¹ "[Security Chiefs Fail to Justify Regulation Spending](#)", Paul Muncaster, Financial Director Magazine, United Kingdom, 19 Sep 06
- ² "[Cyber Security and Information Infrastructure Research Workshop](#)", Dr. Frederick T. Sheldon, Computational Sciences and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, TN, 23 Mar 07
- ³ Peter Drucker, quoted in "[Intelligent Sustainment and Renewal of Department of Energy Facilities and Infrastructure](#)", Chapter 4, Infrastructure Management Performance Measures, Committee on the Renewal of Department of Energy Infrastructure, Board on Infrastructure and the Constructed Environment, Division on Engineering and Physical Sciences, National Research Council of the National Academies, International Standard Book Number 0-309-54652-4, Copyright 2004 by the National Academy of Sciences. All rights reserved.
- ⁴ "[Gartner: Security Costs Fall With Good Policies](#)", by Jeremy Kirk, IDG News Service, 18 Sep 06.
- ⁵ "[The Thickness of Concrete on the Maginot Line](#)", Published by Infowar.Com & Interpact, Incorporated, with permission from The Honorable Paul A. Strassmann, (former) Director of Defense Information, U.S. Department of Defense. Undated.