

ROI Comparison Paper

By Marcia Mealy

Introduction

This paper will compare and contrast 2 major methodologies for ROI discussed in the lecture. ROI or return on Investment is a very important element of any report to Management. For InfoSec reporting, the ROI should show the costs of the security program, if it was successful and it is providing the functionality that was expected. The first methodology is the Gerald Kovacich model by Dr. Gerald L. Kovacich. The second is 'ALE and Risk Assessment'.

ROI Methodologies

The Gerald Kovacich Model is an Informal model based on InfoSec metrics. The first metric is based on two InfoSec drivers, which are the number of systems which fall under the review of the InfoSec Program, and the number of users of the systems. It uses quantitative, statistical, and/or mathematical analyses to measuring InfoSec functional trends and workload or the level of effort (LOE). First each InfoSec function must be identified. Next the driver for the function must be determined. Lastly a metrics collection process must be established that determines if metrics are really needed. The collection process tries to determine why the statistics should be collected, what statistics will be collected and how, when and who will collect them and from where the statistics will be collected. The information is analyzed and the results used to identify areas where efficiency improvements are needed. In addition, it can be used to determine the effectiveness of InfoSec functional goals as well as used as input for performance reviews of the InfoSec staff. Also, it charts InfoSec service and support to determine if it is meeting its goal and/ or requires improvement. The information is presented to management in charts and graph formats.

ALE is an Insurance ROI model, which stands for Annualized Loss Expectancy or Exposure is an industry accepted standard formula for annualizing loss expectancy for threats. It is uses as part of the Risk Assessment to help determine the cost of loss of an asset when there is no hard data. It helps to determine how much should be spent to cover the asset. Even though, the information is subjective, it presents the loss in monetary terms that management should understand. Management can determine if they will eliminate the risk, transfer the risk by purchasing insurance or, or accept the risk by absorbing the potential losses. ALE consists of the following formula:

$$\begin{aligned} \text{ALE} &= \text{SLE} \times \text{ARO} \\ \text{SLE} &= \text{EF} \times \text{AV} \end{aligned}$$

AV is the value of the asset. EF is the exposure factor or percentage measurement of potential loss. If the value of the asset is multiplied by the exposure value, the product is the single loss expectancy or SLE for one threat event. The Single Loss Expectancy is multiplied by the annual rate of an occurrence (ARO) which gives the Annualized Loss Expectancy.

ROI Comparison Paper

Comparison

Both of the Gerald Kovacich Model and ALE methodologies are similar because they are tools that are used to support many of the ISSO decisions and actions. In addition, both methods are subjective because they are educated guesses.

Contrast

ALE over-simplifies risk assessment because it cannot tell the difference between the risks of a low-frequency, high-impact threat and a high-frequency, low-impact threat. For instance, password violations could have a higher ALE ranking than a fire, because of the difference in frequency. However, the ALE can be useful in determining the return on security investment (ROSI) by subtracting the security investment from the damage prevented. The Gerald Kovacich Model uses information from the work load, headcount, time, etc. in the calculations for its risk assessments. In addition, it covers areas that ALE does not, such as access control, audit trail analyses, compliance inspections, systems' approvals, awareness briefings, and contingency planning/disaster recovery. ALE is geared toward the management of threats, only. The methodology does not lend itself toward non-threat related items.

Conclusion

ALE is a methodology that is useful to measure threats for risk assessments, if the issue with the low-frequency, high-impact threat versus a high-frequency, low-impact threat is addressed. When the security investment is subtracted from the damage prevented, it does provide a measurable ROSI. However, the Gerald Kovacich Model is a complete process for gathering, measuring and reporting metrics on the ROSI to management.

Reference

Berinato, Scott "Finally, a Real Return on Security Spending" Calculating Return on Security Investment. CIO Magazine. (15 Feb. 2002) Retrieved May 22, 2005 from <http://www.cio.com/archive/021502/security.html>
http://www.cio.com/archive/021502/security_sidebar.html

Is Return on Security Investment (ROSI) Impossible? Until now open networks defeat all ROI-based security investment models. Sygate. Retrieved May 22, 2005 from <http://china.sygate.com/solutions/request/ROSI%20Whitepaper.pdf>

Kovacich, Dr. Gerald L. Information Systems Security Metrics Management. Retrieved May 20, 2005 from <http://www.shockwavewriters.com/Articles/GLK/issmm.htm>

Kovacich, Dr. Gerald L. Information Systems Security Officer's Guide. Butterworth-Heinemann. 2003

Peltier, Thomas R. Information Security Risk Analysis. Auerbach Publications. 2001.