
EDUCATION AND TRAINING

A Model to Quantify the Return on Investment of Information Assurance

By
Charley Tichenor
Defense Security Cooperation Agency

[The following views presented herein are solely those of the author and do not represent the official opinions of the Defense Security Cooperation Agency.]

Introduction

This paper explains and demonstrates the structure of a model for forecasting the Return on Investment of Information Assurance (ROIA) Model. This was presented at the Department of Defense (DoD) Defense Security Cooperation Agency's 7th Semiannual Information Assurance Conference on April 19, 2006 in Alexandria, Virginia. This paper focuses on the structure of the proposed model. All numbers are notional, and are in the model only to help illustrate its inner workings. Organizations are encouraged to either use this structure "as is" or modify it, and then populate it with their local variables. This paper will discuss the literature review, the theory behind the model, use notional examples to illustrate how the model works, and follow with interim conclusions and suggestions for future research. The model can be used in one or more ways. It can be used to measure the financial return on investment (ROI) of current information assurance (IA) initiatives, such as firewalls, anti-spyware software, antivirus software. Most importantly, it can be used to forecast the ROI of impending IA initiatives.

Quantifying the ROI for any program is important because it is one indicator of the degree to which a program contributes to the parent organization's strategic plan. It can help prioritize investments. ROI can be used to help quantify an individual's or team's job performance, which can support annual performance appraisal evaluation rating levels. This paper presents a model that can be used to quantify the financial ROIA. Potential users of the ROIA Model are encouraged to either use or modify this structure and populate the variables with their own organization's data, perhaps using an operations research analyst to operate the model and an IA manager to provide the data.

Review of the Related Literature

Two important references apply to this research. The first is the book *The Balanced Scorecard: Translating Strategy into Action*, by Kaplan and Norton, Harvard Business School Press, 1996.¹ The Balanced Scorecard model considers measuring ROI using four categories:

- Financial
- Customer satisfaction
- Improvement of internal processes
- Investment in learning and growth

1. Kaplan and Norton, *The Balanced Scorecard: Translating Strategy into Action*, Harvard Business School Press, Boston, MA, 1996.

The currently formulated ROIA Model only considers the financial category. This is not to downplay any other facet of IA, which locally may be of equal or greater importance. This only means that there is room for future research to improve the ROIA Model to address the ROI of non-financial benefits.

The second reference is the New South Wales Department of Commerce's *Return on Investment for Information Security* model.² The ROIA Model is based on the New South Wales approach although there are particular modifications. For example, Table 1 in this paper is a modified version of the corresponding NSW table, and Table 2 is borrowed with little change although it is used somewhat differently here.

Theory

Financial ROI is a measure of the degree to which a program is beneficial to the organization. Conceptually, it can be calculated as follows.

$$\frac{\$ \text{ Benefits}}{\$ \text{ Costs}}$$

For example, suppose a program costs \$1000, and brings in \$1500. The ROI would be then calculated as:

$$\frac{\$1500 - \$1000 \text{ (i.e., net benefit = \$500)}}{\$1000 \text{ (i.e., cost)}}$$

or 50 percent, a 100 percent ROI is “break even.” The ROIA Model is based on the same principle – benefits compared to costs. However, the model is structured on carefully worded concepts and terms. It is academically sound, but operates from a particular perspective. This will be illustrated with examples.

One IA goal is to either prevent or reduce future incidents of “successful” malicious attacks. Installing countermeasures can help achieve this goal. The ROIA Model is currently based on how well the countermeasures reduce the “repair or replace” costs of forecast future attacks. Countermeasures could include special software such as anti-spyware software, security-related hardware, or IA training. We therefore incorporate the following general concepts into the model.

- Current probabilities of successful attacks
- Costs to repair or replace materiel as a result of successful attacks occurring before countermeasures are installed
- Costs to repair or replace materiel as a result of successful attacks occurring after countermeasures are installed
- Costs of countermeasures to prevent or reduce successful future attacks.
- ROI and financial present values

More specifically, we define the following:

2. New South Wales, Australia, Department of Commerce CIO web page, www.oit.nsw.gov.au/files/7.1.15.ROSI_Calculator_1.2.xls. Model developed for New South Wales by Mr. Stephen Wilson.

- The financial benefits are defined here as the forecast repair or replace cost avoidances due to installation of a countermeasure. Successful attack incidents are reduced.
- The financial costs are defined here as the forecast of the costs to procure the countermeasure, paid now, plus the cost of its annual maintenance, which will be paid in the future.

Therefore, the ROIA is modeled as the below ratio:

$$\frac{(\text{Forecast repair or replace cost "before" countermeasures}) - (\text{forecast repair or replace cost "after" countermeasures})}{\text{Cost of countermeasures}}$$

Forecasting Countermeasure Benefits

Let us forecast the ROIA of a hypothetical system needing four countermeasures for four vulnerabilities. Follow the line of thinking sequence shown in the bullet comments above. Start by addressing the first above bullet by perhaps asking, “What is the likelihood of a malware attack happening to a single computer that would cause a repair or replacement during a given year?” (which is the first vulnerability). We demonstrate assuming a five-year lifespan and a 4 percent discount rate for present value calculations. This and all other assumptions can easily be modified as appropriate.

The ROIA Model is built into an Excel spreadsheet, with the Crystal Ball Monte Carlo Simulation software added-in. Refer to Table 1 (extracted from the Excel spreadsheet) for a set of further assumptions. There are seven degrees of attack likelihood, in column 1. Those frequencies are defined in column 2. For this demonstration, we forecast that the malware attack has a “Low” chance happening at least once per year (column 3) but, on average, 1.93 times per year (column 4).

Likelihood	How Often per Individual Computer?	Number Occurrences per 365 Day Year per Individual Computer		
		At Least	Mean	Statistical Distribution
Negligible	Unlikely to occur	0	0.25	Poisson
Very Low	Between 12 and 24 months	0.5	1.42	Poisson
Low	Between 6-12 months	1	1.93	Poisson
Medium	Between 1-6 months	2	7.04	Poisson
High	Between 1 week and 1 month	12	32.00	Poisson
Very High	Between 1 day and one week	52	155.00	Poisson
Extreme	From 1 to 20 per day, or more	365	500.00	Poisson

How to compute the 1.93. Refer to Figure 1, which is from Crystal Ball. We think that such malware successful attacks will arrive at an individual computer in the same random way that cars arrive at highway toll booths, a poisson arrival pattern (see Table 1 column 5). Crystal Ball requires a “rate” parameter for the Poisson. This is entered as 1.5, which is halfway between the 1 in Table 1’s column 3 for a “Low” and the 2 in column 3 for the “Medium.” The “selected range” has a low value of 1 because we defined a “Low” as happening at least once per year. In theory, it could happen infinitely many times so “+ infinity” is the high value. Given these parameters, Crystal Ball computes the average of this Poisson distribution as 1.93.

Poisson distribution with
Rate = 1.5
Selected range is from 1.0 to infinity

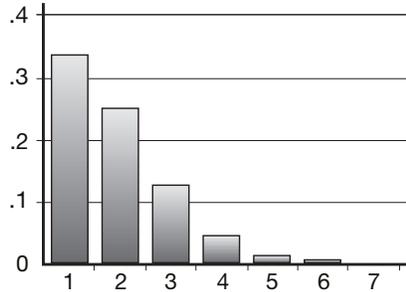


Figure 1. Poisson Distribution of Number of Malware Attacks Per Year.

After forecasting the average (expected) number of occurrences of successful malware attacks per year, we need to forecast the cost to repair or replace equipment affected by those attacks. We use Table 2 as a guideline for assessing the criticality of each attack instance.

Table 2. Criticality per Instance of Successful Attack	
Criticality	Description
Insignificant	Will have almost no impact if threat is realized.
Minor	Will have some minor effect on the asset value. Will not require any extra effort to repair or reconfigure the system.
Significant	Will result in some tangible harm, albeit only small and perhaps only noted by a few individuals or agencies. Will require some expenditure of resources to repair (e.g. "political embarrassment").
Damaging	May cause damage to the reputation of system management, and/or notable loss of confidence in the system's resources or services. Will require expenditure of significant resources to repair.
Serious	May cause extended system outage, and/or loss of connected customers or business confidence. May result in compromise of large amounts of government information or services.
Grave	May cause system to be permanently closed, and/or be subsumed by another (secure) environment. May result in complete compromise of Government agencies.

With this as a guideline, we forecast the cost to repair or replace on an individual basis for each type of successful attack. For this demonstration, we model the criticality of a successful malware attack to be "significant." Specifically, refer to Figure 2, which is from crystal ball. For this demonstration, we model the best-case repair or replace cost situation as \$20. The most likely case is \$150, and the worst case is \$400. This is a triangular distribution, with an average computed by crystal ball at \$190.

Figure 2. Forecast Cost to Repair or Replace Due to a Successful Malware Attack.

Triangle distribution with parameters:

Minimum \$ 20

Likeliest \$150

Maximum \$400

Selected range is from \$20 to \$400

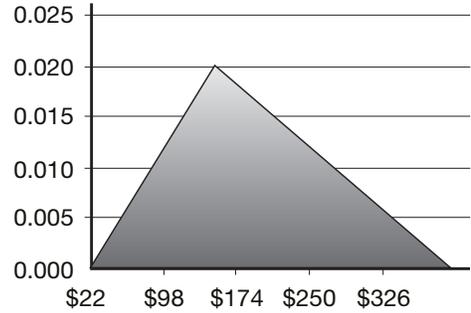


Table 3 from the Excel spreadsheet recaps this. For this vulnerability #1, the Internet Service asset has a vulnerability of significant spyware attack. It has a “Low” likelihood of happening, but if it happens the criticality is considered significant. This should occur about 1.93 times annually per computer in our system, at an average cost of \$190 to repair or replace the computer. For the 100-computer system, this amounts to an annual forecast average cost to repair or replace of \$36,670.

No.	Asset	Vulnerability	Likelihood	Criticality	Before No. Occurrences per Year per Computer	Cost per Incident	Computer	Countermeasures Installed
1	Internet service	Significant spyware attack	Low	Significant	1.93	\$190	100	\$36,670
2	a	aaa	Medium	Insignificant	7.04	\$37	100	\$26,048
3	b	bbb	Low	Minor	1.93	\$103	100	\$19,879
4	c	ccc	Very Low	Damaging	1.42	\$1,133	100	\$160,886
					Total Before Vulnerability Costs ==> \$243,483			

This calculation, however, is deterministic and does not account for the effect of the probability distributions. For example, although the average number of occurrences of successful attacks is 1.93, it could be one in a given year, or two in another year. Instead of multiplying the 1.93 before expected number of occurrences by the \$190 “direct cost per incident” cost to repair or replace (and then by the 100 computers), we could essentially multiply the before occurrences distribution curve by the direct cost per incident distribution curve, and multiply that product by 100, to better picture what actually might happen.

To forecast the expected cost before we buy the countermeasure, the crystal ball selects a random number from the number of malware attacks probability distribution.

- This random number is converted into the actual number of times the threat occurs this year.
- Another random number is selected from the cost to repair or replace probability distribution, and this is converted into the actual repair or replace cost.

- These two values are multiplied together, and then multiplied by the number of computers (100).

This is repeated 20,000 times, i.e., a Monte Carlo simulation run for 20,000 trials, or years. What would the average cost be over this 20,000-year period? Figure 3 below is from crystal ball and shows a histogram plot of the outcomes of each of those 20,000 years (except for a few extreme outliers); it represents the distribution curve of the forecast costs before countermeasures.

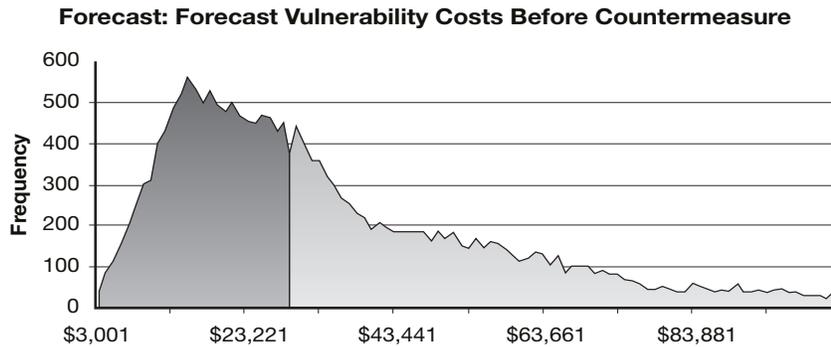


Figure 3: Forecast Vulnerability Costs for a Malware Attack Before Countermeasure Installation.

The Monte Carlo simulation indicates that over the 20,000 years, the possible annual cost to repair or replace for all 100 computers ranges from about \$3,000 to about \$84,000, with an average of about \$28,782. This average value is that where half of the area of the curve is to its left, and half is to its right, and that point can be read directly through crystal ball.

Refer now to bullet 3 above. Assume we now buy a countermeasure. To forecast the average cost to repair or replace after we buy the countermeasure, we multiply the cost to repair and replace by the number of times we expect it to occur and by 100 computers, as shown using Table 4.

Table 4. Calculation of Expected Total After Countermeasures' Installation Repair or Replace Cost.					
After Likelihood	Criticality	After Number Occurrences Per Year Per Computer	Direct Cost Per Incident	Number Computers	Forecast Vulnerability Costs Per Year After Countermeasures Installed
Very Low	Significant	1.42	\$190	100	\$26,980
Very Low	Insignificant	1.42	\$37	100	\$5,254
Negligible	Minor	0.25	\$103	100	\$2,575
Negligible	Damaging	0.25	\$1,133	100	\$28,325
Total "After" Vulnerability Costs ==>					\$63,134

Read across the first data row. For this demonstration for vulnerability #1, the likelihood of a successful malware attack after installation of the countermeasure is modeled as “very low but if it happens the criticality is considered significant. This should occur about 1.42 times annually per computer in our system, at an average cost of \$190 to repair or replace the computer. For the 100-computer system, this amounts to an annual forecast average cost to repair or replace of \$26,980.

As with the before costs, we determine the after costs distribution. Figure 4 shows the after costs simulation results, and they are forecast to average about \$22,581 annually.

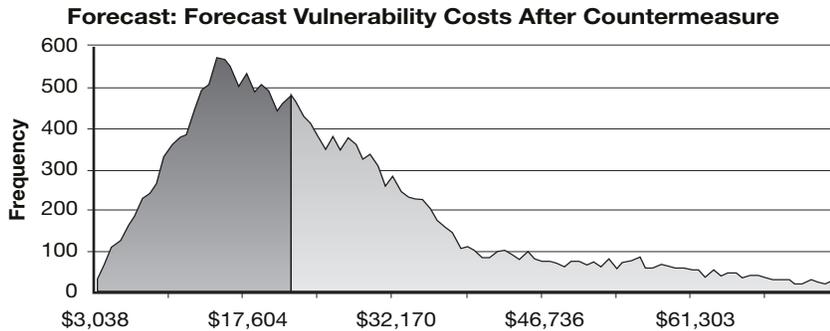


Figure 4. Forecast Vulnerability Costs for a Malware Attack After Countermeasure Installation.

The total five-year before forecast costs are now calculated by simulation. This is the cost of all forecast attacks for the four vulnerabilities, or all four data rows of Table 3. Figure 5 is that total before cost distribution. This average is about \$219,294 for 100 computers.

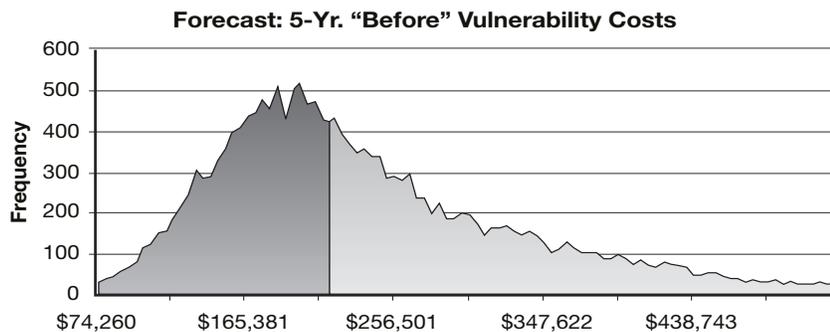


Figure 5. Forecast Vulnerability Costs for all forecast Attacks Before Countermeasures' Installations.

Please note: Table 3 shows the values of the variables after the 20,000th year. The total cost is in the lower right corner cell, showing \$243,283 for that particular year. The model uses the average simulated value of the 20,000 years, or \$219,294.

In like manner, the five-year after forecast costs are calculated by simulation. Figure 6 is the total after cost distribution after the simulation. This average is about \$32,535 for 100 computers. Again, please note that this is different than the total after costs in the lower right cell of Table 4, which was the value of the 20,000th year.

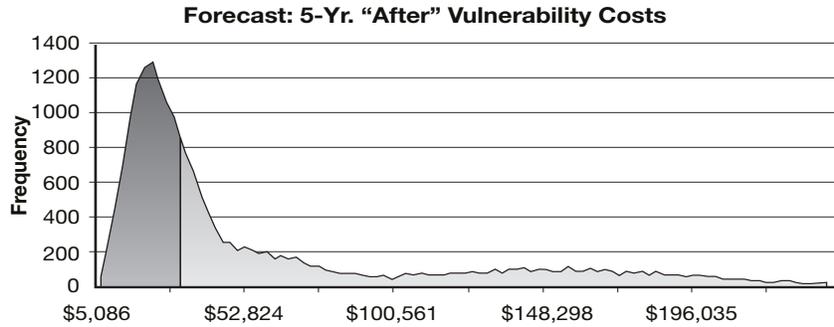


Figure 6. Forecast Vulnerability Costs for all forecast Attacks After Countermeasures' Installations.

To compute the approximate total five-year lifespan benefit, or cost avoidance, we essentially subtract a total of five after simulated cost curves from a total of five before simulated cost curves. The average benefit, or cost avoidance, is about \$874,837, as shown in Figure 7.

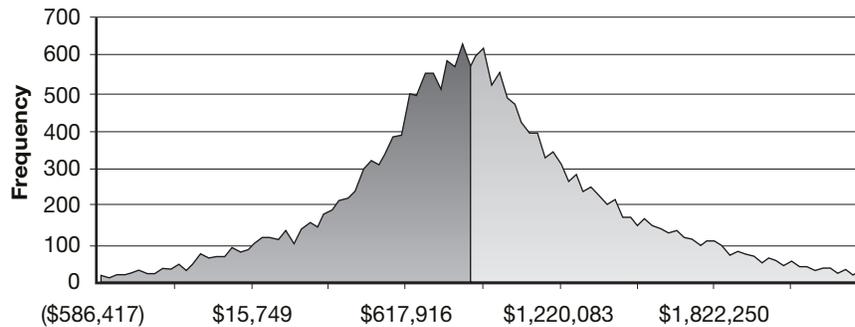


Figure 7. Forecast Average Cost Avoidance for All Forecast Attacks After Countermeasures' Installations.

Forecasting Countermeasure Costs

It is now necessary to model the costs of the countermeasures (reference bullet 4 above). In this demonstration, there are four software countermeasure products installed. Each has an up front purchase price cost, and each has annual maintenance. Refer to Table 5. Assume that these countermeasures will be good for five years each (this year and the four subsequent years). The lower right corner cell is the sum of the five-year life span costs, or \$98,200. This is known with certainty by contract and is not simulated.

Table 5: Actual Countermeasure Costs			
Counter Measures	Up-front Cost per Countermeasure	Recurring Annual Cost per Countermeasure Years 2 thru 5	Total Countermeasure Costs
Install anti-spyware software	\$6,000	\$600	\$8,400
AAA	\$20,000	\$2,000	\$28,000
BBB	\$15,000	\$1,500	\$21,000
CCC	\$10,000	\$7,700	\$40,800
Total	\$51,000	\$11,800	\$98,200

Calculating the Return on Investment of Information Assurance

The ROIA is now calculated by simulation (refer to bullet 5 above).

$$\frac{(5 \text{ before vulnerability cost curves}) - (5 \text{ after vulnerability cost curves})}{(5 \text{ years of countermeasures costs})}$$

The Figure 8 simulation shows that it is possible that this program's ROIA could range from about -600 percent to about 1900 percent. However, the expected ROIA in this notional example is 886 percent, and we are about 93 percent sure that the ROIA will be greater than 100 percent.

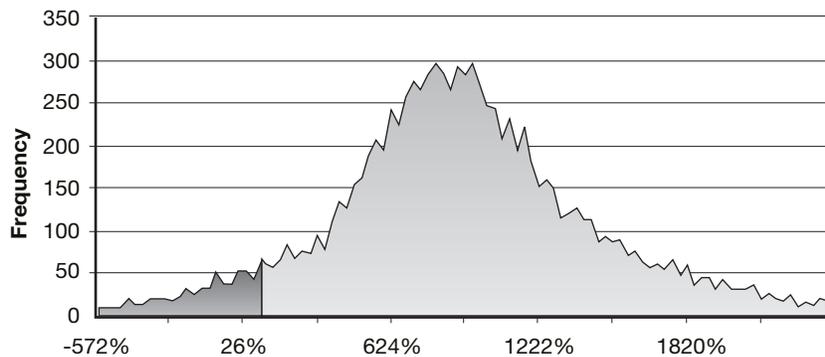


Figure 8. Forecast Five-Year ROIA.

Net Present Value Calculation

Also, this simulation shows that the forecast Net Present Value of this five-year IA program is about \$776,946.

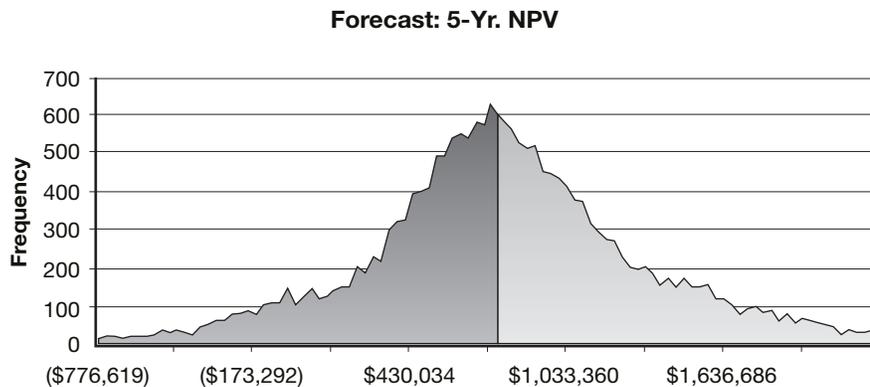


Figure 9. Forecast Five-Year Net Present Value.

Conclusions and Areas for Future Research

A quantitative forecast of an Information Assurance program's value is important to an organization. This model's basic paradigm is that at least a part of the financial ROIA can be quantitatively forecast as a measure of the effectiveness of countermeasures to possible system attacks. This can be formulated as the ratio of future cost avoidances due to those countermeasures to the cost of those countermeasures. This requires using probabilities of current and future successful attacks, costs of countermeasures to prevent or reduce future attacks, probable costs incurred as a result of successful attacks, and Monte Carlo simulations to obtain a distribution of forecast outcomes. The net present value of the IA program can also be forecast.

Although it is possible that an IA program could be justified solely through the financial perspective, future research might focus on ROIA in terms other than financial. For example, the loss of data through a key logger might incur zero cost to repair or replace computers, but might represent a serious security information breach. Which Balanced Scorecard perspective this might fall under, and how to quantify it, might be interesting and valued research.

About the Author

Charley Tichenor, Ph.D., has a Bachelor of Science in Business Administration degree from Ohio State University, a Master of Business Administration degree from Virginia Polytechnic Institute and State University, and a Ph.D. in Business from Berne University. He serves as an Information Technology Operations Research Analyst for the Department of Defense and the Defense Security Cooperation Agency. He also is an Adjunct Professor at Strayer University's Anne Arundel, Maryland campus.