DTEC 6823

Kelly Lucas

Network Administrator

Morgan Stanley

"Economic Evaluation of a Company's Information Security Expenditures"

Abstract

The paper will address why justify security expenditures, what methods have been used within the security industry, what caused the move to justify the security expenditures, and what is the general perception of the information security community and how are they embracing the new methods? The paper will conclude with methodologies that implement ROI, NPV, and IRR to evaluate a company's Information Security Expenditures.

Information Security expenditures are increasingly coming under greater and greater scrutiny. The days of relying on a security guru stating to the CIO "we just need this device" are over. With budgets tightening and profit margins shrinking, the security departments are now competing for capital funds like any other department. Security departments are both struggling trying to manage the risk associated with the e-commerce growth and fighting for their growing budget needs. These stimuli have forced security management to change their persona.

Gordon and Loeb comment in saying; "To protect the confidentiality, integrity, and availability of information, while assuring authenticity and non repudiation, organizations are investing large sums of money in IS activities. Since security investments are competing for funds that could be used elsewhere, it's not surprising that CFO's are demanding a rational economic approach to such expenditures." (Loeb, 2002) In todays security realm, security managers are forced to make a case for the larger expenditures. The journal of security management states, "To ensure adequate IT funding, security must sell management on the potential benefit of the proposed purchases. Security spending is one of the top five IT priorities for 2004, with spending expected to increase 15 to 20 percent this year. But even with companies devoting a larger portion of the IT budget to security initiatives, it is not necessarily sufficient to meet increasing risks. How can IT security officers make the case for the larger expenditures they need?" (6 pg140)

Many different methods and opinions are used for the economic evaluation of security expenditures. For the most part ROI (Return on Investment), NPV (Net Present Value), and IRR (Internal Rate of Return) are the standards. According to Kitteringham and McQuate in 2003, "The most significant factor when attempting to obtain funding is "return on investment," or

ROI. The purse strings will not be loosened until the company knows what it is getting in return for its cash". Others feel that NPV is the gold standard, "A value-added model of computing net present value can give information security specialists what they need to effectively compete."(Somerson, 1994) Gordon and Loeb "show that about a third of CIO's surveyed claim that concepts like net present value are becoming important factors to information-security managers in weighing the costs and benefits of a security investment. More important, many CFO's are starting to require such an analysis from information-security managers as they already do from managers of other organizational subunits." (Gordon and Richardson, 2004). So as can be seen "economists have recently turned their attention toward cybercrime, and now information-security managers are starting to borrow a few tools of the trade."(Gordon and Richardson, 2004). In the past we have relied on fear, uncertainty, and doubt to qualify the expenditures needed to secure an organization. A method or term coined as FUD in the information security community. As you can see, these methods are gradually fading into the past while economic measures are rising to the forefront. "However, according to Earthlink security experts Lisa Ekman and Lisa Hoyt, “Crying wolf may get the first firewall, but over the long run, you need a more well-rounded perspective”(Cavusoglu, Mishra, and Raghura, 2004). Across the field there is a clear movement toward using the economic metrics mentioned above. ""I go to security conferences where we sit around puzzling about what kind of metrics to use for measuring the results of security programs," says Adam Stone, a security management analyst for the financial-services industry. "The metrics we have right now for assessing vulnerability and for measuring the effectiveness of our investments are all based on subjective judgments. They're fundamentally flawed." He says we can learn from the methods of financial, statistical, economics, and securities professionals who deal with these kinds of uncertainties all the time to

predict and measure business effectiveness in a rational way."(Gordon and Richardson, 2004).

So far we have established the answer to why justify security expenditures and briefly examined how we have moved to using ROI, NPV, and IRR. One might ask what has pushed upper management to requiring this form of economic evaluation onto what was previously considered a cost. Security is not a new concept, thieves have been exploiting vulnerabilities since the beginning of time. Organizations have responded to these vulnerabilities equally as long . The need to justify the expenditures is not necessarily a new concept. The security industry has simply grown to the point it needs to express itself in the same language as the c-level management. However, there are other factors in the economy that have stimulated this movement. First, if we evaluate the movement of the economy since 2000 we have seen little to no growth overall. Dow on 10/21/2000 equaled 10,226. Dow in 2005 equaled 10,215 on 10/21/2005 (Marketwatch) Secondly, a change in the way companies conduct business. E-commerce has grown tremendously causing security departments to be creative in the methods of securing the organization while keeping in line with tightening budgets and reduced profits. In trying to keep one step ahead of the current vulnerabilities, they have been busy trying to secure new funds. "Return on Security Investment (ROSI) has become a controversial topic due to immense growth of e-businesses." (Cavusoglu, Mishra, and Raghura, 2004). When these factors are coupled together it becomes clear why the upper management is requiring detailed explanation of how and why the security department is spending funds.

What is the general perception of the information security community and how are they embracing the new methods? Bruce Schneier, security expert and author of *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (Copernicus Books, 2003), says, "Economics—not technology—determines what security technologies get used. These days, I

feel like I do more economics than computer security."(Gordon and Richardson, 2004). Overall the infosec community has realized some approach must be used regardless of the method. One unique perception I ran across was documented in the Computer Security Journal that basically suggested a wait and see approach. "One explanation for the ubiquitous nature of information security breaches may be that it is economically rational to initially invest a portion of the information security budget and defer remaining investments until security breaches actually occur. In other words, by deferring the decision to invest the remaining $1 million, the revelation of actual security breaches provides a clearer picture of whether or not to spend the discretionary funds. Although actual losses are expected to occur while waiting for such revelations, the expected benefits of waiting outweigh the costs. Regardless of how the information security budget is initially derived, it may be economically sound to wait for actual breaches to occur before allocating all of the funds available for information security activities." (Gordon, Loeb, and Lucyshyn, 2003). Information Week quoted Gordon and Richardson in saying "Information-security managers need to view security through the lens of economics as well as a technical-security lens if they want to successfully carry out their jobs and level the playing field during budget requests. The sooner information security managers realize this fact, the better off all of us will be in terms of cybersecurity".(1pg56) Steve A. Purser in Computers and Security feels "....as information security is a business issue. Those organizations that do not recognize this will probably find it harder to sensibly balance new business opportunities against the associated risks, which will reduce their competitiveness and ultimately affect profitability.(Purser, 2004). I feel Palmer wraps this issue in the Journal of Security Management in saying, "The question for security department directors, then, is how to demonstrate financial return to the entire organization. The answer combines solid performance data and standard financial analysis

tools." (Palmer, 2004). In researching the question of the security fields perception I find that majority of the industry has begun to embrace the economic metrics to validate the security department expenditures by expressing them in terms of ROI, NPV, and IRR. The 2005 CSI/FBI Computer Crime and Security Survey State "A significant number of organizations conduct some form of economic evaluation of their security expenditures, with 38 percent using Return on Investment (ROI), 19 percent using Internal Rate of Return (IRR) and 18 percent using Net Present Value (NPV).

So far we have answered the questions of: why justify security expenditures, what methods have been used within the security industry, what caused the move to justify the security expenditures, and what is the general perception of the information security community and how are they embracing the new methods? Next we will take a look at the methods and an example of how the methods are being used.

Let us begin with Return on Investment (ROI). ROI as it names implies simply defines how much will I receive for what I have spent. If I spend 10 dollars and receive 100 dollars then I have an ROI of 900%. ROI is expressed as the net gain divided by the initial investment. In the simplest of terms:

$$\frac{\text{(What I gained total) - (What I invested to create the gain)}}{\text{(What I Invested)}}$$

EX. $\frac{100 - 10}{10}$

$= 9$ or 900%

Even though this is such a simple formula, much debate has been created in applying this to security expenditures. First, let us consider the initial investment. What we spend to secure the

network is easy enough to calculate. Simply total all funds spent including such things as:

- Cost of equipment (Firewalls, IDS, Proxy servers, etc)
- Cost of administration (Per hour cost of all security activity- install eq, configure eq, update eq, review security logs, incident response handling, disaster recovery, etc...)
- Overhead (utilities, facility cost to house staff and eq)

What a company invest is considered tangible or hard assets. This investment has been calculated for years in numerous organizations. A valid number can be generated quite easily. The problem lies in determining a number for what is gained. Firewalls simply do not generate revenue, IDS do not generate revenue. So the gain becomes a subjective number, thus lies the problem. How do we assign gain to the mitigation of risk. We also have to consider the gain of not relinquishing private information of the company or our clients. "Softer still and even harder to estimate is a security breach's collateral damage, including litigation fees, fines for information disclosure, and harm to the company's overall image and brand."(Pisello, 2004). Some in the information community consider this as a problem in examining soft and hard dollars. The soft dollars being the assignment of gain to the above mentioned attributes of risk mitigation, reputation and so forth. "This issue of soft versus hard benefits does not invalidate the security business case, but it does make it unique. While almost all business cases include both hard and soft benefits, most of the important benefits with security business cases are soft."(Pisello, 2004). "Security's biggest challenge is how to measure the value of prevention for the purposes of ROI."(Kitterham and McQuate, 2003).

Let us consider a few of these soft dollars and recommend a method for assigning a dollar figure to these assets. One way to assign the value to risk mitigation is to examine the cost of each individual threat within an organization. For example one might look at a DOS attack and

find data to support the cost of such an attack at a similar company. Let us assume the average cost of a DOS is 100,000 dollars for a similar company. Let us also assume a DOS attack occurs once every two years. From this data we can determine the annual loss expectancy(ALE) would be $50,0000 dollars. 100,000/2 = 50,000 Hence we use $50,000 as the gain attributed to the device that mitigates the risk. Now this is only as accurate as the data accumulated to establish this $50,000 figure. There are websites and resources such as www.securitystats.com/sspend.html, Carnegie Mellon's www.cert.org/stats/cert_stats.html, CSI's CSI/FBI 2005 Computer Crime and Security Survey that can assist in attaining tangible figures. Moving on to the softer dollars of reputation and loss of business the company suffers is even more subjective. However, a method that can be used is to evaluate the data available about similar companies and how each successful attack has affected their bottom line.
The above mentioned websites are helpful also in attaining this information. In trying to determine accurate numbers nothing can substitute data generated by your own company. Accurate records need to be kept of attacks before and after the implementation of any new security solution. As time goes forward the security community will accumulate more an more data to help validate the subjective methods used in calculating the ROI.

In addition to the subjective downside of ROI, the time attribute presents a problem and leads managers to using Net Present Value along with ROI to justify security expenditures. "If you consider money's time value, then it's quite possible for an investment to have a less rosy assessment under a net-present-value model than a simple one-year computation of ROI. Of course, the reverse may be true, especially for projects that provide multiple years of benefit. The point is that net present value, which is consistent with the notion of maximizing the value of a firm, compares apples with apples over the entire life of an information-security investment.

In contrast, ROI is based on an accrual system of accounting and is short-term in focus."(Gordon, 2004)

NPV is very useful in evaluating between alternatives. The methodology behind NPV is to find the after tax cash flows generated by a particular solution and find what those cash flows are worth in todays dollars. The cash flows will consist of the initial investment, cost of installation, cost of configuration, cost of maintenance and updates. Below I will give an example and walk through the process of calculating NPV using excel.

You are considering a new IDS system to enhance security. The IDS will cost $75,000 to install and configure. Annual maintenance and associated operating costs are $25,000. The system is expected to mitigate an annual loss expectancy (ALE) of $150,000 dollars. There is no salvage value of the system. The combined tax rate is 35%. The minimal acceptable rate of return (MARR) for your firm is usually 50%. In other words the company expects to make 50% on their money if invested in some other task. If the project cannot overcome this hurdle of 50% then we do not want to implement the project. The MARR is intentionally set high to help compensate for the subjective savings of the ALE. Do you recommend this investment?

I will use an after tax analysis to determine the NPV of this project opportunity and use straight-line depreciation and a five-year life for this alternative.

See Chart Below

1. BTCF Real Dollars = this is the exact amount of money received or money paid without accounting for any inflation. In the beginning of the project we will pay $75,000 dollars. Each year we will save in an additional $150,000 dollars in ALE.

2. I assumed an inflation rate of 3% for the cost of IDS maintenance. The project does not state the ALE will rise with inflation so the ALE will remain constant throughout the life of the project. As you can see from the chart below I have inflated the IDS maintenance by 3% each year.

3. BTCF Actual dollars = this is the actual worth of the savings after IDS maintenance (inflated 3% per yr) is deducted. If we did not consider the inflation of maintenance this would still be expressed in Real dollars.

4. Straight-line depreciation is figured by the following formula:

Depreciation/yr = (first cost- salvage value)/Project life

$75,000/5yrs = $15,000

5. Taxable income is calculated by subtracting the depreciation from the BTCF actual dollars. This is the actual amount of money we will pay taxes on.

6. The combined tax rate was given as 35%

7. Taxes paid are calculated by multiplying the taxable income by the combined tax rate.

8. ATCF is calculated by subtracting the taxes paid from the BTCF actual dollars. From this we can now calculate the NPV to determine the validity of the alternative.

9. Net Present Value is calculated from the ATCF using the NPV function inside Excel. Achieving a positive $74,142 dollars lets us know that we are exceeding our exaggerated hurdle rate or MARR of 50%. So yes, we should invest in the project.

IDS System	75,000											
ALE savings	150,000											
IDS Maintanance	25,000											
No Salvage												
MARR	50%											
Combined tax rate	35.00%											
Inflation of Expense	3%											
Year	BTCF Real $	IDS Maintanance	Inflation Rates	Inflated expense	BTCF Actual $	Straight-line Depreciation	Taxable Income	tax rate	Taxes paid	ATCF		
0	($75,000.00)				($75,000.00)					($75,000.00)		
1	$150,000.00	$25,000.00	1	$25,000.00	$125,000.00	($15,000.00)	$110,000.00	0.35	$38,500.00	$86,500.00		
2	$150,000.00	$25,000.00	1.03	$25,750.00	$124,250.00	($15,000.00)	$109,250.00	0.35	$38,237.50	$86,012.50		
3	$150,000.00	$25,000.00	1.03	$26,522.50	$123,477.50	($15,000.00)	$108,477.50	0.35	$37,967.13	$85,510.38		
4	$150,000.00	$25,000.00	1.03	$27,318.18	$122,681.83	($15,000.00)	$107,681.83	0.35	$37,688.64	$84,993.19		
5	$150,000.00	$25,000.00	1.03	$28,137.72	$121,862.28	($15,000.00)	$106,862.28	0.35	$37,401.80	$84,460.48		
									NPV	$74,142.00		

As with ROI, NPV also has a subjective or soft dollars within the calculation. However, I proposed a solution is to exaggerate the MARR. By exaggerating the MARR we are saying that even if we could make 50% returns on our money the project would still be considered a viable solution.

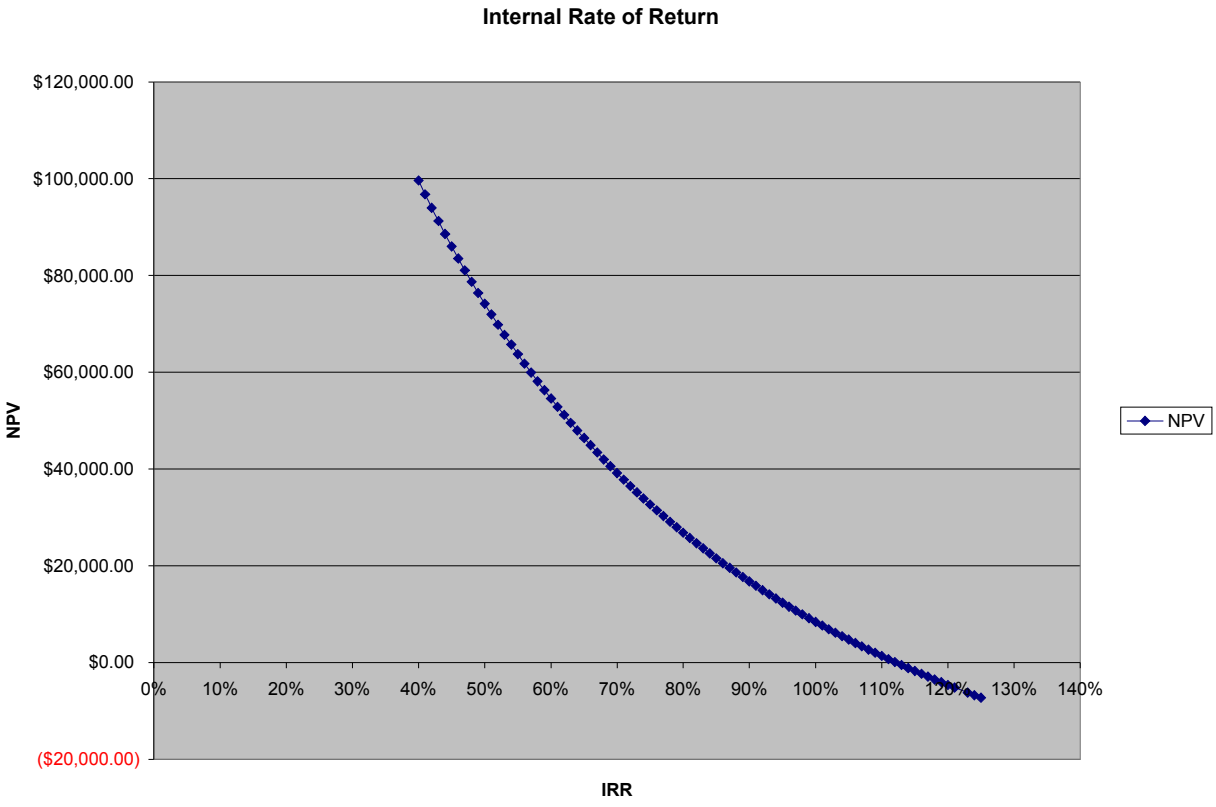
Internal Rate of Return (IRR) is the final economic metric discussed that a security manager might use to evaluate a project expenditure. The IRR is calculated by using a cash flow like NPV. Unlike the NPV calculation IRR will show a security manager at what rate will we break even. Considering the example of NPV above we will use the ATCF and excel to calculate the IRR.

Using the above cash flows we find an IRR of 112.15%. The data below clearly shows the point where the NPV = 0. IRR is a method for evaluating the feasibility of this project. In simple terms we are looking for an IRR to be greater than the MARR set by the project. As you can see the IRR of return analysis yield an IRR of 112.15% clearly above the MARR of 50%. You can also find the exact point were the Net Present Value equals zero. This will show the IRR or in other words the point were the present worth of the cash inflow equals the present worth of the cash outflow. According to our example a company would have to invest their money and make a return of 112.15% before it could substantiate a better return than buying the IDS system.

Initial Investment	Year 1	Year 2	Year 3	Year 4	Year 5	IRR
($75,000.00)	$86,500.00	$86,012.50	$85,510.38	$84,993.19	$84,460.48	112.1505%

IRR	NPV
40%	$99,660.85
41%	$96,774.01
42%	$93,969.33
43%	$91,243.66
44%	$88,594.03
45%	$86,017.57
46%	$83,511.58
47%	$81,073.44
48%	$78,700.70
49%	$76,390.97
50%	$74,142.00
51%	$71,951.62
52%	$69,817.77
53%	$67,738.46
54%	$65,711.82
55%	$63,736.01
56%	$61,809.31
57%	$59,930.07
58%	$58,096.67
59%	$56,307.60
60%	$54,561.40
61%	$52,856.66
62%	$51,192.03
63%	$49,566.22
64%	$47,977.99
65%	$46,426.14
66%	$44,909.54
67%	$43,427.08
68%	$41,977.70
69%	$40,560.39
70%	$39,174.17
71%	$37,818.10
72%	$36,491.26
73%	$35,192.80
74%	$33,921.87
75%	$32,677.66
76%	$31,459.40
77%	$30,266.33
78%	$29,097.72
79%	$27,952.89

80%	$26,831.17
81%	$25,731.89
82%	$24,654.44
83%	$23,598.21
84%	$22,562.61
85%	$21,547.10
86%	$20,551.11
87%	$19,574.13
88%	$18,615.65
89%	$17,675.18
90%	$16,752.24
91%	$15,846.38
92%	$14,957.15
93%	$14,084.12
94%	$13,226.88
95%	$12,385.03
96%	$11,558.18
97%	$10,745.94
98%	$9,947.97
99%	$9,163.90
100%	$8,393.39
101%	$7,636.11
102%	$6,891.74
103%	$6,159.97
104%	$5,440.50
105%	$4,733.03
106%	$4,037.28
107%	$3,352.98
108%	$2,679.86
109%	$2,017.65
110%	$1,366.12
111%	$725.00
112%	$94.08
113%	($526.89)
114%	($1,138.13)
115%	($1,739.85)
116%	($2,332.27)
117%	($2,915.59)
118%	($3,490.01)
119%	($4,055.72)
120%	($4,612.92)
121%	($5,161.78)
123%	($6,235.21)
124%	($6,760.11)
125%	($7,277.37)



ROI, NPV, and IRR can all benefit from accurate records being kept. "The security team should keep a log of breaches and their costs, and use this data to build the business case". (Pisello, 2004). Each of the methods have their own unique problems. ROI has the difficulty in defining what is gain. NPV and IRR both have the quandary of figuring the ALE. As can be demonstrated raising the expectation of the MARR can help in mitigating the risk of an overestimated ALE. According to Cavusoglu, Mishra and Raghura in 2004, "The purpose of IT security infrastructure is to mitigate the risk up to a point where the marginal cost of implementing controls is equal to the value of additional savings from security incidents." Even

with the problems of these metrics "mitigated risk is in many senses the primary deliverable of the information security process. In other words, *the information security process adds value to the enterprise by reducing the level of risk that is associated with its information and information systems*. A reduced risk profile is obviously of value to the enterprise and should therefore be seen as a return on the investment that made this possible."(Purser, 2004)

In conclusion I have shown what methods have been used within the security industry, what caused the move to justify the security expenditures, and what is the general perception of the information security community and how are they embracing the new methods. In addition I have shown examples of how ROI, NPV, and IRR can be used to evaluate a company's Information Security Expenditures.

References

Cavusoglu, H., Mishra, B., Raghunathan, S. (2004). A model for evaluating IT security investments. *Association for Computing Machinery. Journal of Communications of the ACM* 47. page 87.

Gordon, L., Loeb, M. (2002). Return on information security investments: Myths vs. realities. *Journal of Strategic Finance 84*. pp.26-32.

Gordon, L., Loeb, M, Lucyshyn, W. (Spring, 2004). Information security expenditures and real options: A wait-and-see approach. *Computer Security Journal 19* (2). pp. 1.

Gordon, L., Richardson, R. (March 29, 2004). The new economics of information security. *Information Week 982*. pp.53-57.

Gordon, L., Richardson, R. (April, 2004). The new economics of information security. *Optimize* (30).

Kitteringham, G., McQuate, C. (September, 2003). Many happy returns. *Security Management*. *47 (9)*. pp.121.

Marketwatch. Big Charts, Dow Jones Industrial Average Historical Quotes. Retrieved October 24, 2005 from http://bigcharts.marketwatch.com/historical/default.asp?detect=1& symbol= djia& close_date=10%2F21%2F2000&x=51&y=28

Palmer, W. (March, 2004). What's security worth? *Security Management 48 (3)*. pp. 53-56.

Pisello, T. (October, 2004). Is there a business case for IT security? *Security Management 48 (10)*. pp. 140-142.

Purser, S. (October, 2004). Improving the ROI of the security management process. *Journal of Computers & Security 23 (7)*. pp. 542-546.

Somerson, I. (October, 1994). Information: What it costs when it's lost. *Security Management 38 (10)*. pp. 61-65.