Return on information security investments: Myths vs. realities

Article · January 2002

2 authors, including:

Martin P. Loeb
University of Maryland, College Park

RETURN ON

INFORMATION SECURITY INVESTMENTS

Myths vs. Realities

BY LAWRENCE A. GORDON AND MARTIN P. LOEB

Information security (IS) breaches are a growing concern. In fact, 90% of the respondents in a recent survey of private and public organizations conducted by the Computer Security Institute and the FBI had detected security breaches in the previous year.

To protect the confidentiality, integrity, and availability of information, while also assuring authenticity and nonrepudiation, 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 CFOs are demanding a rational economic approach to such expenditures.

One increasingly popular metric for capturing the cost-benefit aspect of information security is the return on information security investments, also known as return on security investments, or ROSI. Chief information officers (CIOs) as well as CFOs are embracing it, but its strengths and weaknesses aren't well understood, which has led to confusion and misuse. To clarify, let's examine some myths and realities.

ILLUSTRATION: VICTORIA KANN


$NPV = \sum_{t=1}^{n} \frac{CF_t}{(1+k)^t} - Cost$
IRR = 43%
$Cost = \sum_{t=1}^{n} \frac{CF_t}{1+IRR}$
IRR = 43%
$(1+IRR)^2$
ROI =
$(1+IRR)^2$
IRR = 43%
$NPV = \sum_{t=1}^{n} \frac{CF_t}{(1+k)^t} - Cost$
$Cost = \sum_{t=1}^{n} \frac{CF_t}{1+IRR}$

Myth 1: The accounting concept of "return on investment" is an appropriate concept for evaluating information security investments.

A cursory reading of articles and books could lead you to believe that the notion of accounting return on investment, or ROI (accounting income divided by accounting asset value), is valid for evaluating investment decisions. That isn't the case.

Reality: The accounting ROI concept is not equal to a true economic rate of return, so it shouldn't be used to evaluate investments.

The economic rate of return, usually called the internal rate of return (IRR), is the appropriate metric for evaluating investments, including information security investments. As most financial professionals know, there's no simple procedure for converting ROI to IRR.

The irreconcilable differences between ROI and IRR stem from the fact that accounting notions of income and asset values are based on historical (*ex post*) accrual and nondiscounted concepts. In contrast, economic notions of income and asset values are based on future (ex ante) risk-adjusted discounted cash flows.

The IRR can be expressed in this equation:

$$Cost = \sum_{t=1}^{n} \frac{CF_t}{(1+IRR)^t}$$

where,

CF_t = net cash flow in period t,

Cost = Cost of investment,

n = economic life of investment.

Advocates of the ROSI concept should be using the economic notion of IRR, rather than the accounting notion of ROI, for evaluating information security investments.

Myth 2: Maximizing the IRR on information security investments is an appropriate objective.

On the surface, it seems logical to presume that a firm with a higher internal rate of return is doing better than a firm with a lower internal rate of return. Indeed, inferences suggesting that a firm should try to maximize its overall return on investments (including information security-related investments) are common.

Reality: Trying to maximize a firm's IRR on security investments isn't appropriate.

Say an organization estimates its annual expected loss due to security breaches is going to be $2 million in the first year and $800,000 in the second year. These amounts are derived by multiplying the dollar value associated with potential breaches by the probability that each breach will occur. Now suppose the firm estimates that with an initial incremental investment of $1 million in upgrading the information security system, it can reduce the annual expected loss due to security breaches to $700,000 and $500,000 in years one and two, respectively.

Panel A of Table 1 shows the expected cost savings from the security investment would be $1,300,000 in the first year and $300,000 in the second year. The firm decides that if it doesn't upgrade its security system today, it will upgrade it in two years.

The ROSI is computed by solving Equation 1 for the IRR [i.e., $1,000,000 = $1,300,000/(1+ IRR) + 300,000/(1+ IRR)^2]. The projected IRR is 50%. Assuming the firm estimates its cost of capital to be 14%, the investment seems financially attractive.

An alternative would be to buy a more sophisticated system for $1,400,000 (see panel B). Although it costs more, it would do a better job of preventing security breaches. The loss is expected to be $200,000 in the first year and $513,000 in the second year, so the expected savings are $1,800,000 the first year and $287,000 the second year. The IRR would be 43%, compared to 50% for the initial opportunity.

Since the goal should be to generate the maximum net benefits—not the highest IRR—the alternative security investment is the better option. In other words, the goal should be to generate the maximum net present value (NPV), which is equivalent to maximizing the present value of net benefits, as defined in our next equation:

$$NPV = \sum_{t=1}^{n} \frac{CF_t}{(1+k)^t} - Cost$$

where,

k = the cost of capital; CF_t and n are defined in the equation under Reality 1.

Consider the net benefits of these two opportunities:

◆ The initial investment opportunity (panel A) results in a present value of $371,191.

◆ The alternative (panel B) results in a net present value of $399,785.

Assuming the firm can obtain the funds, the larger alternative investment is the one it should choose.

Since the lifespan of new technology is so short, let's now assume the firm will upgrade its information securi-

Table 1: RETURN ON SECURITY INVESTMENT

Panel (A)

Initial Incremental Information Security Investment = $1,000,000

	YEAR 1	YEAR 2
Security Breach without Incremental Investment	$2,000,000	$800,000
Security Breach with Incremental Investment	700,000	500,000
Savings from Security Investment	$1,300,000	$300,000

$$\$1,000,000 = \$1,300,000/(1+IRR) + \$300,000/(1+IRR)^2$$

IRR = 50%

$$NPV = [\$1,300,000/(1+.14) + \$300,000/(1+.14)^2] - \$1,000,000 = \$371,191$$

Assuming the project has a one-year life:

IRR = ($1,300,000/$1,000,000) – 1 = 30%

NPV = $1,140,351 – $1,000,000 = $ 140,351

Panel (B)

Alternative Incremental Information Security Investment = $1,400,000

	YEAR 1	YEAR 2
Security Breach without Incremental Investment	$2,000,000	$800,000
Security Breach with Incremental Investment	200,000	513,000
Savings from Security Investment	$1,800,000	$287,000

$$\$1,400,000 = \$1,800,000/(1+IRR) + \$287,000/(1+IRR)^2$$

IRR = 43%

NPV = $1,799,785 – $1,400,000 = $ 399,785

Assuming the project has a one-year life:

IRR = ($1,800,000/$1,400,000) – 1 = 29%

NPV = $1,578,947 – $ 1,400,000 = $ 178,947 ty system in one year instead of two. The initial security investment opportunity would have an IRR of 30% and NPV of $140,351. The alternative investment would have an IRR of 29% and NPV of $178,947.

Once again, the investment with the highest NPV isn't the same as the one with the highest IRR. Choosing the security investment with the highest IRR won't maximize the net benefits. Even assuming a one-year life, the alternative investment is better.

Myth 3: IRR and NPV are *ex post* metrics for evaluating the actual performance of information security investments.

The actual performance evaluation of investment decisions is an historical process. Many believe that IRR and NPV are in line with that process.

Reality: IRR and NPV are *ex ante* metrics.

Whether you have a one-year or two-year horizon, it's important to note that the economic rate of return (IRR) is computed on an *ex ante*, or anticipated, basis. If a company wants to evaluate the actual performance of an investment, it needs to do this on an *ex post* basis. In other words, it needs to compare the actual (*ex post*) cost savings from the security investment to the anticipated (*ex ante*) cost savings. Such a comparison is often referred to as "post-auditing."

Post-auditing is difficult because the benefits of specific investments aren't easily separated from other activities within a company. This is particularly relevant to security investments; the more successful the project, the less likely you are to see breaches.

Thus, on an *ex post* basis, it's extremely difficult to assess the accuracy of the original estimates of cost savings from security investments. The same is true for evaluating an *ex post* NPV.

Myth 4: It's appropriate to invest in security activities up to the level where the investments equal the expected loss from security breaches.

On the surface, this seems to make sense. But this approach stems from a misunderstanding of the basic marginal revenue vs. marginal cost concepts for maximizing profits.

Reality: Firms should invest substantially less in information security than the expected loss from security breaches.

As security investments increase, there's strong reason to believe the net benefits from preventing breaches may initially increase but will eventually decline. In deriving an optimal strategy for a firm that's trying to maximize the NPV of security investments, it's necessary to consider the relationship between the level of investment and the decrease in the probability of a security breach. This can be summarized as a "security breach probability function."

For example, assume that a loss associated with a security breach is $1 million and the initial probability of the breach occurring is 0.4. The expected loss from the information security breach is $400,000. (The data points making up the security breach probability function are shown in Table 2.)

Based on Table 2, an investment of $25,000 in information security would lower the probability of a breach to 0.3, an investment of $50,000 would lower the probability to 0.25, and so forth. If the firm were to invest the full amount of the initial expected loss, $400,000, the expected loss from a breach would decline to $1,000. Thus, the firm would be spending $400,000 to reduce the expected loss by $399,000.

By investing up to the expected loss, the firm should expect to see profits decline by $1,000. You can easily see that if the firm had stopped investing at a level of $100,000 (where the expected marginal benefits from additional investment are still greater than the marginal cost of that investment), it would have spent $100,000 to reduce the expected loss from a breach by $270,000, producing a positive net benefit of $170,000.

Although it's beyond the scope of this article, we have developed a model—called the GLEIS™ model—that provides managers with a framework for analyzing the appropriate level of investment related to information assurance. It takes into account a company's risk exposure as well as the cost associated with reducing this exposure. Using this model, we discovered that the optimal level of investment in security-related activities should not exceed approximately one third of the potential expected loss.

This provides a ballpark upper bound to consider. The optimal spending level from our example, $100,000, falls in this area. Firms would be far better served if they focused on deriving an optimal level of security investments instead of pursuing a rate of return.

THE SUM OF ALL PARTS

Remember these four points:

◆ First, the accounting and economic rates of return are *not* interchangeable. Discussions about the return on

Table 2: SECURITY BREACH PROBABILITY FUNCTION

(A) Investment in Information Security	(B) Probability of a Security Breach	(C)=$1,000,000 x (B) Expected Loss
$ 0	0.4	$400,000
$ 25,000	0.3	$300,000
$ 50,000	0.25	$250,000
$ 75,000	0.2	$200,000
$100,000	**0.13**	**$130,000**
$125,000	0.11	$110,000
$150,000	0.09	$ 90,000
$175,000	0.07	$ 70,000
$200,000	0.06	$ 60,000
$225,000	0.055	$ 55,000
$250,000	0.05	$ 50,000
$275,000	0.03	$ 30,000
$300,000	0.01	$ 10,000
$325,000	0.008	$ 8,000
$350,000	0.006	$ 6,000
$375,000	0.003	$ 3,000
$400,000	**0.001**	**$ 1,000**
$425,000	0.0007	$ 700
$450,000	0.0004	$ 400
$475,000	0.0002	$ 200
$500,000	0.00001	$ 10

security investments need to be clear as to which return is being discussed.

◆ Second, even when discussing the economic rate of return (which most agree is preferred), it isn't appropriate to try and maximize this metric.

◆ Third, when discussing the actual performance of information security investments, a careful distinction needs to be made between *ex post* and *ex ante* measures.

◆ Fourth, and finally, companies would be better served if they pursued the notion of deriving an optimal level of information security investment instead of pursuing some sort of rate of return. ■

For more information on this subject, read

L.A.Gordon, *Managerial Accounting: Concepts and Empirical Evidence*, McGraw-Hill, New York, N.Y., 2000.

L.A. Gordon and M.P. Loeb, "The Economics of Investment in Information Security," *ACM Transactions on Information and System Security*, November 2002.

NIST (National Institute of Standards and Technology), "An Introduction to Computer Security," *The NIST Handbook, Special Publication 800-12*, 1995.

Lawrence A. Gordon and Martin P. Loeb are on the faculty of the Robert H. Smith School of Business at the University of Maryland, College Park. Gordon, an Ernst & Young Professor of Managerial Accounting and Information Assurance, can be reached at (301) 405-2255 or lgordon@rhsmith.umd.edu. Loeb, a professor of Accounting Information and Information Assurance and Deloitte & Touche Faculty Fellow, can be contacted at (301) 405-2209 or mloeb@rhsmith.umd.edu.

Support for their research was provided in part by the DoD, Laboratory for Telecommunications Sciences, through a contract with the University of Maryland Institute for Advanced Computer Studies.