Return on information security investments: Myths vs. realities

Article : January 2002

CITATIONS
49

READS
236

2 authors, including:

Martin P. Loeb
University of Maryland, College Park
60 PUBLICATIONS 4,707 CITATIONS

All content following this page was uploaded by Martin P. Loeb on 28 April 2016.
The user has requested enhancement of the downloaded file.
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.
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 undiscounted 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., \( $1,000,000 = \frac{1}{(1 + IRR) + 300,000}/(1 + IRR)^2 \)]. 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)

<table>
<thead>
<tr>
<th>Security Breach without Incremental Investment</th>
<th>Year 1</th>
<th>Year 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2,000,000</td>
<td>$800,000</td>
<td></td>
</tr>
<tr>
<td>Security Breach with Incremental Investment</td>
<td>700,000</td>
<td>500,000</td>
</tr>
</tbody>
</table>

Savings from Security Investment

$1,300,000

$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)

<table>
<thead>
<tr>
<th>Security Breach without Incremental Investment</th>
<th>Year 1</th>
<th>Year 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2,000,000</td>
<td>$800,000</td>
<td></td>
</tr>
<tr>
<td>Security Breach with Incremental Investment</td>
<td>200,000</td>
<td>513,000</td>
</tr>
</tbody>
</table>

Savings from Security Investment

$1,800,000

$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
Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
### Table 2: Security Breach Probability Function

<table>
<thead>
<tr>
<th>Investment in Information Security</th>
<th>Probability of a Security Breach</th>
<th>Expected Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0</td>
<td>0.4</td>
<td>$400,000</td>
</tr>
<tr>
<td>$25,000</td>
<td>0.3</td>
<td>$300,000</td>
</tr>
<tr>
<td>$50,000</td>
<td>0.25</td>
<td>$250,000</td>
</tr>
<tr>
<td>$75,000</td>
<td>0.2</td>
<td>$200,000</td>
</tr>
<tr>
<td>$100,000</td>
<td>0.13</td>
<td>$130,000</td>
</tr>
<tr>
<td>$125,000</td>
<td>0.11</td>
<td>$110,000</td>
</tr>
<tr>
<td>$150,000</td>
<td>0.09</td>
<td>$90,000</td>
</tr>
<tr>
<td>$175,000</td>
<td>0.07</td>
<td>$70,000</td>
</tr>
<tr>
<td>$200,000</td>
<td>0.06</td>
<td>$60,000</td>
</tr>
<tr>
<td>$225,000</td>
<td>0.055</td>
<td>$55,000</td>
</tr>
<tr>
<td>$250,000</td>
<td>0.05</td>
<td>$50,000</td>
</tr>
<tr>
<td>$275,000</td>
<td>0.03</td>
<td>$30,000</td>
</tr>
<tr>
<td>$300,000</td>
<td>0.01</td>
<td>$10,000</td>
</tr>
<tr>
<td>$325,000</td>
<td>0.008</td>
<td>$8,000</td>
</tr>
<tr>
<td>$350,000</td>
<td>0.006</td>
<td>$6,000</td>
</tr>
<tr>
<td>$375,000</td>
<td>0.003</td>
<td>$3,000</td>
</tr>
<tr>
<td>$400,000</td>
<td>0.001</td>
<td>$1,000</td>
</tr>
<tr>
<td>$425,000</td>
<td>0.0007</td>
<td>$700</td>
</tr>
<tr>
<td>$450,000</td>
<td>0.0004</td>
<td>$400</td>
</tr>
<tr>
<td>$475,000</td>
<td>0.0002</td>
<td>$200</td>
</tr>
<tr>
<td>$500,000</td>
<td>0.0001</td>
<td>$10</td>
</tr>
</tbody>
</table>

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


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.