Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA)

Marco Cremonini
Dipartimento di Tecnologie dell'Informazione
University of Milano
26013 Crema, Italy
cremonini@dti.unimi.it

Patrizia Martini
Zucchetti.com
26900 Lodi, Italy
patrizia.martini@zucchetti.com

Abstract

Producing a cost-benefit analyses of security solutions has always been hard, because the benefits are difficult to assess and often only a part of the overall cost is clear. Despite this, today the provision of economic evaluations of security technology investments is a requirement that more and more customers ask vendors to satisfy. In this paper, we consider the typical calculation of a Return-On-Investment (ROI) index based on the evaluation of the Annual Loss Expectancy (ALE), as the one provided usually by vendors of IT security. Our motivating assumption is that such classical index, the ROI, provides a partial characterization of investments in information security technology, because it lacks to explicitly consider attackers' behavior. We suggest that to better evaluate security technology investments, the ROI index should be coupled with a corresponding index aimed at measuring the convenience of attacks, the Return-On-Attack (ROA) expecially in situation where different technologies are combined or where the possible degradation of a security solution's efficiency over time must be taken into account.

1 Introduction

The importance of information security increased enormously in the last few years in the consideration of customers of information technology (IT) solutions. It is sufficient to walk into a kiosk to find out that all IT publications have now a security-related section and dozen of different magazines dedicated to IT security are available. IT security importance has also driven new investments: statistics show that almost the totality of firms have antivirus and firewalls in place and a large number of organizations have developed projects aimed at protecting their assets from information security threats. However, it has been often also observed that this increase of information security expenditures was driven mostly by emotional reactions to new perceived risks rather than by pragmatic cost-benefit analyses of the available solutions.
One of the problems that security managers must tackle is to provide a right evaluation of different security plans and to estimate costs and benefits of technologies without having tangible data. Security technology benefits depend on how often an attack is expected, which damage is likely to occur and how effective the security technology is in mitigating the damage caused by attacks. Communication gaps between security managers and IT managers have been often reported, resulting in decisions that do not fully take into account both the economic convenience and the technical effectiveness.
The discipline studying the economics of information security technology investments has already provided some relevant results and analyses [1, 2, 4, 5, 6], although probably not yet well understood and accepted in the large. In this context, our work is motivated by observing that many vendors seem now aware of the necessity of providing an economic justification of the costs of their solutions, instead the analyses that often are provided appear severely incomplete and sometimes misleading. In particular, ROI-based evaluations, the ones usually provided, in our opinion suffer of many weaknesses and are intrinsically incomplete. In this paper we propose an approach to improve ROI-based evaluations by integrating them with a new index, called Return-On-Attack (ROA), aimed at measuring the convenience of attacks. The ROA index reflects the average and supposed impact of a security solution on attackers' behaviors. The goal is to identify the solution that mostly discourage attackers in their intrusion attempts, an aspect that the usual ROI analysis does not identify clearly.

4th Workshop on the Economics on Information Security 2005

2 Return-on-Attack (ROA)

In our analysis, we started from the typical calculation of a Return-On-Investment (ROI) index, based on the evaluation of the Annual Loss Expectancy (ALE), the expected efficiency of adopted security solutions and their corresponding costs. The cost-benefit model presented by Wei *et al.* [7] and Foster [3], for example, like many other studies, has considered such elements applied to information security technologies and has modeled the ROI index as follows:

$$\text{ROI} = \frac{ALE_{beforeS} - ALE_{afterS}}{cost\ of\ security\ measure} = \frac{EFF * CI - CS}{CS} = \frac{EFF * CI}{CS} - 1$$

The relation can be derived starting from a security measure S and estimating $ALE_{beforeS}$, which represents the annual costs related to all security incidents that the security measure S is well-suited to mitigate. We call CI these annual costs, and then $ALE_{beforeS}$ equals CI . These costs may include both tangible and intangible losses, such as costs for data recovery, in the first case, or damage to the reputation, in the second. The term ALE_{afterS} is composed by two parts. The first one is the annual cost that the firm still suffers from security incidents that security measure S should have been able to avoid, but actually did not. This term is calculated as the difference between losses before the adoption of security measure S, that is $ALE_{beforeS}$, and the fraction of these losses saved due to the adoption of S. That fraction, called EFF, with EFF included in [0,1], represents the *efficiency* of security measure S, and the savings on losses are then represented by $EFF * ALE_{beforeS}$. The second part

of ALE_{afterS} is the cost of the security measure *S*, called *CS*.
Our motivating assumption is that such classical index, the ROI, provides a partial characterization of investments in information security technology, because it lacks to explicitly consider attackers' interests. Assuming that the organization's loss is equal to the attacker gain is often a gross simplification. Also, the cost of an attack cannot be directly related to the cost of the security measure because different solutions at different costs might be perceived as equally expensive to break from the attacker's viewpoint.
To this end, we suggest that to better evaluate security technology investments, the ROI index should be coupled with a corresponding index aimed at measuring how the attacker's convenience changes with the adoption of the same security measure *S*. We have called it *Return-On-Attack* (*ROA*) and it is defined as the gain the attacker expects from a successful attack over the losses that he sustains due to the adoption of security measure *S* by his target. In this definition of *ROA*, the expected gain due to a successful attack is the independent term that we assume to be constant. The dependent term is the cost of the attack that may vary. It is important to highlight that the ROA is the evaluation an organization does about the effectiveness of a security measure in discouraging a certain class of intrusion attempts assuming some profiles of potential attackers. This means that it does not exactly correspond to the ROI calculated by a specific attacker in the evaluation of his investment. The two perspectives are not necessary the same, although both largely based on perceptions about costs, gains and efficacy.
Similarly to the *ROI* calculation, we call *GI* the expected gain from the incident, *CA* the perceived cost sustained by the attacker to succeed and $EFF^{'}$ the efficiency of the attacker to violate security measures. We can then state that:

$$\text{ROA} = \frac{gain\ from\ successful\ attack}{cost\ before\ S + loss\ caused\ by\ S} = \frac{GI}{CA_{beforeS}+(CA_{afterS}-CA_{beforeS})}$$
$$= \frac{GI}{\frac{CA}{EFF^{'}_{beforeS}}+(\frac{CA}{EFF^{'}_{afterS}}-\frac{CA}{EFF^{'}_{beforeS}})} = \frac{GI}{\frac{CA}{EFF^{'}_{afterS}}}$$

We make the following assumption:
The attacker's efficiency to violate security measures corresponds to the inability of security measures to impair his attacks. Thus, for a security measure S with efficiency EFF, the attacker's efficiency $EFF^{'}$ *is equal to 1-EFF.*
Then, we correlate *ROA* with the efficiency *EFF* of *S*:

$$\text{ROA} = \frac{GI}{\frac{CA}{EFF^{'}}} = \frac{GI}{\frac{CA}{1-EFF}} = \frac{GI}{CA} * (1-EFF)$$

¿From the attacker's viewpoint, *ROA* must be maximized. Consequently, from the defender's viewpoint, aiming at evaluating investment in security measure *S*, the *ROA* must be minimized.

3 Using ROI and ROA

Let us now show how the conjunction of ROI and ROA could improve the evaluation of IT security investments. In particular, we will present cases where the ROI alone could lead to ambiguous results. Although our cases are purposely tailored to stress negative consequences, we believe they actually represent models of real situations. Two aspects concerning ROI are stressed:

- ROI alone helps understand whether an investment provides for a positive return, but does not permit to compare two solutions, both yielding a positive ROI, based on the *disadvantages* they provide to attackers;
- After the adoption of a technology, and the positive evaluation of the corresponding investment, the context may change for several reasons, both technical and economic. The ROI does not take into account *compensations* between the cost of a security solution and its efficiency, which may result in unchanged ROI values but different efficacy and convenience of the solutions.

For instance, consider the following simplified case study with two potential solutions for contrasting script kiddies: hardened operating systems and an host-based intrusion detection system (HIDS). Assume that EFF_{HOS}, the efficiency of hardening OSs (HOS), is 75%, while the EFF_{HIDS} is 33%. The annual cost of intrusion due to script kiddies is $1.000, the cost of the HIDS is $300 and the cost of HOS is $100.

$$ROI_{HOS} = \frac{0.75*1000}{CS_{HOS}} - 1 = \frac{750}{CS_{HOS}} - 1 = 1.5$$
$$ROI_{HIDS} = \frac{0.33*1000}{CS_{HIDS}} - 1 = \frac{333}{CS_{HIDS}} - 1 = 2.33$$

According to this example, the HIDS will be chosen over HOS. Let's look at corresponding ROA by approximating the term $\frac{GI}{CA}$ with the number *N* of intrusions. Suppose $N = 10$.

$$ROA_{HOS} \widetilde{=} N * (1-EFF) = N * 0.25 = 2.5$$
$$ROA_{HIDS} \widetilde{=} N * (1-EFF) = N * 0.66 = 6.6$$

Even with this gross estimation, we can observe that the different efficiency in discouraging attackers may lead to different conclusions with respect to the only ROI analysis. What the ROI does not capture is the *difference between mitigating the effects of attacks and discouraging attackers by making their efforts no longer profitable*. In the first case, the attacker's target still remains profitable but with a reduced margin and he may be pushed to pay more (i.e. attacking more frequently, with more sophisticated techniques, or looking for different vulnerabilities) for raising his gain. In short, an attacker may suffer losses but at the same time be encouraged to act more efficiently. In our example, the HOS solution results in a ROA of 2.5, meaning that the attacker could gain just two hosts for his purposes. This sensible reduction with respect to the situation before hardening OSs could induce the attacker to change his target instead of paying more.
This simple example let us introduce another aspect that involves the ROI analysis: the *modifications in the environment* with respect to the time of the ROI evaluation and how these modifications could be compensated in the ROI analysis. Consider again the ROI formula and a certain ROI value, say ROI_{t_0} the one calculated at time t_0 when a security solution *S* was chosen. One goal of investments is that their convenience do not decrease over time with respect to the time of the evaluation (at least within a certain time frame). Thus, we want that the value ROI_{t_0} will remain constant. However, the same value ROI_{t_0} could be obtained at following time t_1 either because the values of *EFF*, *CI* and *CS* are unchanged or as a result of *compensations*. For example, if $EFF_{t_1} = \frac{1}{2} * EFF_{t_0}$ and $CI_{t_1} = CI_{t_0}$, and $CS_{t_1} = \frac{1}{2} * CS_{t_0}$, then $ROI_{t_1} = ROI_{t_0}$. This example, although over-simplified, points out a problem of ROI and of security technology investments evaluation: *the effectiveness of security technology investments could degrade due to context changes without affecting the ROI index*.
For instance, consider a firewall appliance and suppose that at time t_0 it resulted the better choice according to a ROI analysis, providing a high efficiency, say 90%. At time t_1, following a management decision that esteemed too high the costs payed, for example because due to firewall security policies it became more difficult to provide new interacting services, the firewall policy has been made less restrictive (a situation that happens quite often, as documented by Wool [8]). Is the firewall investment still convenient at time

t_1? With the simplifications assumed before, $EFF_{t_1} = \frac{1}{2} * EFF_{t_0}$ and $CS_{t_1} = \frac{1}{2} * CS_{t_0}$, the ROI is unchanged, so the management decision seems to have preserved previous invesments. Look at the ROA, instead, by assuming that $\frac{GI}{CA}$ is constant between t_0 and t_1, $EFF_{t_0} = 90\%$ and $1 - EFF_{t_1} = 1 - \frac{1}{2} * EFF_{t_0}$:

$$\text{ROA}_{t_0} = \frac{GI}{CA} * 0.1$$
$$\text{ROA}_{t_1} = \frac{GI}{CA} * (1 - \frac{1}{2} * EFF_{t_0}) = \frac{GI}{CA} * 0.55$$

The convenience to attack the organization increased more than 5 times as a consequence of a management decision that the ROI could not capture.
Finally, consider the case of a technology that is added to a previous one and look at the ROI and ROA indexes. For example, we assume that the previously discussed HOS solution has been applied, as decided at time t_0 ($CI_{t_0} = 1000$, $CS_{HOS} = 300$, and $EFF_{HOS} = 75\%$). At time t_1, the adoption of a new firewall appliance ($CS_{FW} = 100$ and $EFF_{FW} = 90\%$) is decided. The loss CI that the firewall mitigates is the residual part resulting from the previous adoption of the HOS solution: $CI_{t_1} = 1000 - 0.75 * 1000 = 250$. Thus, ROIs are:

$$\text{at time } t_0\text{: ROI}_{HOSt_0} = \frac{0.75*1000}{300} - 1 = 1.5$$
$$\text{at time } t_1\text{: ROI}_{FWt_1} = \frac{0.9*250}{100} - 1 = 2.25$$

The ROI_{FWt_1} seems to confirm that the adoption of the firewall in addition to the previous hardened OS solution is positive. However, this result might not represent the real situation. For instance, if the firewall is deployed at network perimeter, as usual, then it now represents the first line of defense against attackers, followed by an inner layer represented by hardened OSs. Hence, ROI evaluation changes since it is the firewall investment to be evaluated with respect to the full *ALE* (e.g. 1000) and the investment in hardening OSs with respect to the residual costs for intrusions (e.g. $1000 - 0.9 * 1000 = 100$):

$$\text{at time } t_1\text{: ROI}_{FW} = \frac{0.9*1000}{100} - 1 = 8$$
$$\text{and ROI}_{HOS} = \frac{0.75*100}{300} - 1 = -0.75$$

As a result, the investment in HOSs seems no longer convenient, according to the ROI. As a consequence, it seems that the HOS should be dismissed in favour of the firewall alone. Look at ROA:

With FW only: $\text{ROA}_{FW} = \frac{GI}{CA} * (1 - \text{EFF}_{FW}) = \frac{GI}{CA} * 0.1$

With FW and HOS:
$\text{EFF}_{FW/HOS} = \text{EFF}_{FW} + (1\text{-}EFF_{FW}) * EFF_{HOS} = 0.975$
$\text{ROA}_{FW/HOS} = \frac{GI}{CA} * (1 - \text{EFF}_{FW/HOS}) = \frac{GI}{CA} * 0.025$

The ROA seems to confirm that the HOS solution provides just a small benefit because it is applied to marginal attacks that escape firewall filtering. Then, the small utility and negative convenience of the HOS could be the conclusion reached by freezing this scenario at a certain time. However, we have already observed that it should be taken into account that the efficiency of a certain solution could easily *decrease over time*. Recall the scenario seen before when the efficiency of the firewall decreased to 45% due to a management decision and ROA raised to 0.55. Look at the same case with the addition of the HOS solution:

With FW only: $EFF_{FW} = 45\%$ $ROA_{FW} = \frac{GI}{CA} * 0.55$

With FW and HOS:
$EFF_{FW/HOS} = EFF_{FW} + (1\text{-}EFF_{FW}) * EFF_{HOS} = 0.86$
$ROA_{FW/HOS} = \frac{GI}{CA} * (1\text{-}EFF_{FW/HOS}) = \frac{GI}{CA} * 0.1375$

The presence of the HOS, although it resulted not convenient according to the ROI index and providing few benefits according to the first calculation of the ROA, proved to be important as a *second line of defense* because it permits to keep the total efficacy (i.e. $EFF_{FW/HOS}$) of the security architecture at a good 86%, despite the drop of the firewall efficacy from 90% to 45%. As a consequence, the ROA calculated after the firewall's efficacy dropped, shows just a small increase, from 0.1 to 0.1375, instead of jumping to 0.55 as without the hardened OS protection.

4 Conclusion

The principal consideration of this work is that the ROI alone is unable to catch the different impact that solutions have on attackers' behaviors and do not take into account the variations of security solutions efficiency due to technical or management reasons. To this end, we have discussed some case studies, which, although extremely simplified and far from a comprehensive description of real scenarios, should help and encourage to extend ROI analyses to provide better evaluations of security technology investments.
In future works we want to examine in greater details the different case studies in order to provide more precise models, for examples of script kiddies or spammers. Game theory could certainly help to refine our analysis. Moreover, the availability of statistical data and analyses of attackers behavior could be fundamental for better evaluations. The area of Honeypot/Honeynet could be one important source of information.

5 Acknowledgements

This work was supported in part by the European Union within the PRIME Project in the FP6/IST Programme under contract IST-2002-507591 and by the Italian MIUR within the KIWI and MAPS projects.

6 References

[1] ANDERSON, R. J. Why information security is hard - an economic perspective. In *Proc. of the 17th Annual Computer Security Application Conf.* (2001).

[2] CAVUSOGLU, H., MISHRA, B., AND RAGHUNATHAN, S. A model for evaluating it security investments. Tech. rep., University of Texas at Dallas, School of Management, 2002.

[3] FOSTER, S., AND PACI, B. Analysis of return on investment for information security. Tech. rep., Getronics Inc., 2002.

[4] GORDON, L. A., AND LOEB, M. P. The economics of information security investment. *ACM Transactions on Information and System Security 5*, 4 (2002), 438–457.

[5] GORDON, L. A., LOEB, M. P., AND LUCYSHYN, W. Information security expenditures and real options: A wait-and-see approach. *Computer Security Journal 19*, 2 (2003), 1–7.

[6] SCHECHTER, S. E. *Computer Security Strenght & Risk: A Quantitative Approach*. PhD thesis, Harvard University, 2004.

[7] WEI, H., FRINKE, D., CARTER, O., AND RITTER, C. Cost-benefit analysis for network intrusion detection systems. In *Proc. of the 28th Annual Computer Security Conf.* (2001).

[8] WOOL, A. A quantitative study of firewall configuration errors. *IEEE Computer* (June 2004), 62–67.