Return on Security Investment – Pros and Cons

Chanakya Gaur

EN.650.653.01 – Financial Issues in Managing a Secure Operation

Information Security Institute, Johns Hopkins University

5.1 There have been numerous media articles and academic research papers on the topic of Return on Security Investment (ROSI). No matter what methodology is used to calculate the ROSI, there will always be a level of uncertainty. Please write a paper that discusses the pros and cons of the ROSI calculation. Please include in your discussion how intangibles are addressed within the information security field in general and specifically as it relates to the ROSI.

Abstract

The concept of Return on Investments(ROI) is applied to every investment in every type of organization. It is no surprise that ROI is calculated for security expenses as well. The executives of a company want to be aware of the impact that is caused due to the expenditure for security in the firm. The European Network and Information Security Agency (ENISA) developed a model to calculate the Return on Investment for security investments in organizations. Calculating a Return on Security Investment(ROSI) can inform executives how much the firm should implement security in the most cost-effective way. However, measuring a ROSI can prove to be difficult as it involves events which may or may not occur. The fact that most of the times, security is not a revenue generating department, usually brings up the question as to how many resources should be invested effectively, if required at all. In this essay, we shall discuss the process to calculate Return on Security Investments, the factors that influence ROSI, its advantages and disadvantages and future developments in calculating ROSI.

Keywords: Investment, Security, ROI, ROSI

Return on Security Investment – Pros and Cons

The Chief Information Security Officer (CISO) must usually submit a ROSI calculation to the CEO for significant investments. This can be a challenge as it needs to be prepared in a way that requested resources are approved and the credibility of CISO is maintained. Since security is not revenue generating most of the times, its business value in terms of company reputation and other intangible aspects need to be highlighted. Let us first see the how ROSI is calculated.

# Calculating ROSI

There are a few concepts which form the basis of ROSI calculation:

**Single Loss Expectancy (SLE)[[1]](#footnote-1)**

SLE is the expected amount of financial loss for a single security incident. This includes cost of both, the data assets and indirect assets.

**Annual Rate of Occurrence (ARO)**

ARO is the probability or likelihood of a security incident occurring in a organization for a year.

**Annual Loss Expectancy (ALE)**

ALE is the total amount of expected financial loss to an organization due to security incidents in a year.

**Mitigated Annual Loss Expectancy (mALE)**

mALE is the amount that is left after subtracting the amount of financial loss prevented in ALE due to security implementations.

Hence, ROSI is defined as “Implementing an effective security solution lowers the ALE: the more a solution is effective, the more reduced is the ALE.”[[2]](#footnote-2).

As defined by ENISA, formula for calculating ROSI combines the quantitative risk assessment and the cost of mitigating risks. The formula is:

Calculating ROSI can be a challenging task for the one authoring it. The author of the ROSI should be aware of all the information assets, risks, business impact and their counter measures so that the ROSI can contain information learnt from past experiences and predict the likelihood of the attacks for the next year. The author of ROSI should also include certain assumptions such as:

* Knowing that threats are evolving continuously, the author must consider that the value of know threats is low and must also to prepared for unknown threats and their impact.
* Possible threats due to vulnerabilities in new products or process.

ROSI is important as any security breach will not only impact the information technology department but will also have an impact on other factors of the company such as financial loss, legal implications, loss of reputation and even loss of productivity. Until the breach is diagnosed, worked upon and contained, the incident cannot be considered contained and the impact to the company may last until the incident has been dealt with. There are not just financial loses for the data compromised but also additional financial loss such as legal fees and cost to recover data compromised. There is an additional consequence of involving law enforcement, regulations departments and maybe even specialized team depending upon the level of severity of the incident. Not to mention the impact a security incident may have on the reputation of a company, it may cost the company a lot of funds to come up with strategies to restore their reputation unless the company has already been compromised to level that it has to shut down. Financial losses are also involved in all the steps of dealing with a security incident which is detection, containment, correction and recovery.

# Advantages of ROSI

ROSI clearly has a few advantages. Firstly, it increases the efficiency of the company. Calculating ROSI will help the company to utilize their resources in a more directed format to increase productivity. For example, if the ROSI calculated of the next year estimates that possible risks to the company have reduced, the company can focus the security team to monitor only the new threats and reduce energy spent on irrelevant threats. This will ensure that minimum resources are utilized optimizing the operational expenses of the company. This will also free some of the company resources which can be used to develop new products or enhance research which would improvise their position in the market. Secondly, it also helps quantify, even if not accurately, but estimate the approximate costs and possible threats the company may face and needs to be prepared for. It is better for a company to have some estimation about the threats that they face and the amount of resources they might need to mitigate them. ROSI is also important for companies that do not directly deal in information technology development, such as banks, courier services and insurance to protect themselves from brutal attackers on the internet and make them better prepared for security breaches.[[3]](#footnote-4)

Looking at the advantages, one thing we can observe is that calculating ROSI isn’t enough but the company’s culture towards “Risk” of a security occurrence is important as well. Risk is an intangible value and quantifying it into a ROSI is part of Risk Culture. Risk Culture consists of aspects like Risk Tolerance, Risk Avoidance and Risk Appetite.[[4]](#footnote-5) Risk Appetite is the amount of risk a company is willing to take to allow a security breach to occur. Ideally, we wouldn’t want a company to have a high-risk appetite if it deals with sensitive information. Risk Tolerance is the amount of risk a company can sustain before it majorly affects the company or its users to a level that the company may have to shut down. Risk Avoidance is the blaming and learning done by the company before they take effective action against a threat. Using ROSI and the company’s risk culture, graphs can be plotted which will help allocating and estimating the cost needed for effective security for the company.

However, ROSI does come with its disadvantages. Let’s discuss some prominent cons of ROSI.

# Disadvantages of ROSI

ROSI is calculated on multiple approximations. The cost required to manage security incidents and the loss may vary at times. The calculations are solely based on the perception of the accessor and can be biased towards an interest. These calculations are more towards justifying a decision rather than derive to it. Statistical data is also an essential part to estimate possible threats. However, since most companies would rather hide security breaches to protect their reputation, actuarial statistical data is not easily found. Additionally, ROSI cannot completely answer some questions such as the argument that security does not generate direct revenue, the security investment may not be cost-effective and the fact that there is no foolproof way of determining the optimal cost for security investments. Reasons that ROSI cannot answer these questions are:

* There is no standard or uniform method for working to ensure profitability
* Their benefits are dependent on the amount of security incidents occurred and mitigated which cannot be predicted accurately
* There is clearly a difficulty in quantifying the benefits that security investments yield

Another disadvantage of ROSI is that it is more expensive as compared to investing more for bug-free software development. It is better to develop bug free software rather than spend on correcting it. Thus, companies prefer investing more for development and tend to neglect security. However, developing completely bug free code is not easily achievable and examples for that are the Société Générale bank which lost US $ 6.6 Billion due to imperfect controls and management supervision and the wiring problem of Airbus A380 which costed the company US $6.4 Billion. These examples prove that saving money regardless of cost is not always effective.[[5]](#footnote-6)

# Future Developments in ROSI

Since ROSI is its initial phases, multiple attempts are being made to increase the financial profitability of the model by evaluating the cost of security more accurately. Some the models that have been developed are:

## The Hummer Model:7

This model is developed by Hua Qiang Wei from the University of Idaho which basically consists of a box in which the network traffic is logged. This traffic has been passed through a firewall before entering the box. The box will segregate suspected malicious traffic and develop patterns. It will also generate reports which can be studied by the security team and can be further investigated. According to this model, it is cost effective to use intrusion detection systems compared to other security mechanisms. Through this model, companies can better calculate the cost of detecting an attack and counting the frequency of attacks more definitely.

## The Hoover Model:[[6]](#footnote-7)

The Hoover Model was developed by Massachusetts Institute of Technology and @Stake, a company based in Boston. In this model, a database of information on the vulnerabilities and security threats of software is maintained. This database is used to achieve maximum return on their security investment. The companies participating in this model mainly develop software and collaborate their research to understand how they can better protect their products.

## The CMU Model:7

This model is a quantitative study by Carnegie Mellon University which has developed a theory on how much the investment on security should be increased to reach optimal security investment. The study is based on a regression analysis conducted on attack data from CERT. This model manages investigated attacks that occurred and their frequency, how much a certain type of attack affected a certain type of company and the damage it could cause. Using this data, a model was generated to simulate attacks on make believe companies to test the model.

# Conclusion

From this essay, we have seen that even through calculating return on investment is a standard practice in most companies for activities that involve preparing or predicting the future, calculating return on security investment is still in its early stages and has a lot of uncertain parameter which make it unreliable. Since there is not a lot of data from the past to study, developing a foolproof model to calculate ROSI has proven to be difficult. It is true that ROSI has its own advantages and its need to access optimal investments for security in companies in necessary, however, with the limitations involving intangible benefits and high costs, the model needs to be further developed so that the parameters are quantifiable; allowing calculation of ROSI to be more accurate. An accurate ROSI would help companies to access optimal cost for security investments, thus saving resources and minimizing risk as much as possible. Nevertheless, one thing is for sure, given the increase in security incidents occurring with companies, a rise in investment is necessary to protect them from the brutal side of the internet.

1. *Kohen, I. (2018). How to calculate your return on security investments. CSO Online. Retrieved 6 March 2018, from https://www.csoonline.com/article/3229887/security/how-to-calculate-your-return-on-security-investments.html* [↑](#footnote-ref-1)
2. *ENISA, “Introduction to Return on Security Investment”, December 2012,* [*https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment/at\_download/fullReport*](https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment/at_download/fullReport) *(accessed March 6, 2018)* [↑](#footnote-ref-2)
3. *Christer Magnusson, Josef Molvidsson and Sven Zetterqvist,“Value creation and Return on Security Investment”* [↑](#footnote-ref-4)
4. *Gelbstein, E., (2015). Return on Security Investment – 15 Things to Consider. Available at: https://www.isaca.org/Journal/archives/2015/Volume-1/Pages/Return-on-Security-Investment-15-Things-to-Consider.aspx* [↑](#footnote-ref-5)
5. *Gelbstein, E., (2015). Return on Security Investment – 15 Things to Consider. Available at: https://www.isaca.org/Journal/archives/2015/Volume-1/Pages/Return-on-Security-Investment-15-Things-to-Consider.aspx* [↑](#footnote-ref-6)
6. *Christer Magnusson, Josef Molvidsson and Sven Zetterqvist,“Value creation and Return on Security Investment”* [↑](#footnote-ref-7)