Introduction to Return on Security Investment

Helping CERTs assessing the cost of (lack of) security

[Deliverable – December 2012]

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu

Follow us on Facebook Twitter LinkedIn YouTube & RSS feeds

Contact details

To contact ENISA for this report please use the following details:

- E-mail: opsec@enisa.europa.eu
- Internet: http://www.enisa.europa.eu

Contents

1 Executive Summary

As for any organization, CERTs need to measure their cost-effectiveness, to justify their budget usage and provide supportive arguments for their next budget claim. But organizations often have difficulties to accurately measure the effectiveness and the cost of their information security activities. The reason for that is that **security is not usually an investment that provides profit** but **loss prevention**. So what is the right amount an organization should invest in protecting information?

The aim of this document is to initiate a discussion among CERTs to create basic tools and best practices to calculate their Return on Security Investment (ROSI). This key notion is essential when justifying costs engagement and budgets for those entities that deal with security on a regular basis (security departments, CERTs, etc.).

Although the methods outlined here are straightforward, their application to the real world should take into account a general tendency to misevaluate the actual **cost of an incident**, a central notion of the ROSI calculation. While being controversial, the Gordon & Loeb Model[1] is an attempt to ease the finding of the optimal level of investment to protect a given asset.

Due to the diversity of their nature, funding models and capabilities, calculating the return on investment of CERTs has to go beyond a single ROSI calculation. In fact, assessing the cost-effectiveness of CERTs should take into account the **beneficial actions** that CERTs achieve by contributing to detect, handle, recover from and deter incidents early and efficiently. And, the earlier an incident is handled, the less expensive is its mitigation. The profitability of a CERT is therefore assessed by determining the difference of incident handing costs with the help of CERT versus not having a CERT.

[1] *"The Economics of Information Security Investment ", Lawrence Gordon and Martin Loeb, http://ns1.geoip.clamav.net/~mfelegyhazi/courses/BMEVIHIAV15/readings/04_GordonL02economics_security_investment.pdf*

2 The need for ROSI calculation

2.1 Answers to important questions

Return on investment

In every public or private organisation, each budget investment has to be justified and its effectiveness is often evaluated afterward. In finance, this evaluation is called the *Return on investment* or *rate of return*. The ROI is calculated as follow:

$$ROI = \frac{Gain\ from\ investment - Cost\ of\ investment}{Cost\ of\ investment}$$

Example of ROI calculation:

Alice would like to run a lemonade business for summer. She needs money for setting up the business. Bob gives her 200€ to start her business. In return, Alice agrees to give Bob 50% of the benefits.

At the end of summer, Alice made 1000€ of benefits. Bob gets 500€.

Bob's Return on Investment is calculated as follow:

$$ROI = \frac{500 - 200}{200} = 150\%$$

Return on *security* investment

The concept of the ROI calculation applies to every investment. Security is no exception. As stated in ENISA's work program 2012, "executive decision-makers want to know the impact security is having on the bottom line. In order to know how much they should spend on security, they need to know how much is the lack of security costing to the business and what are the most cost-effective solutions."

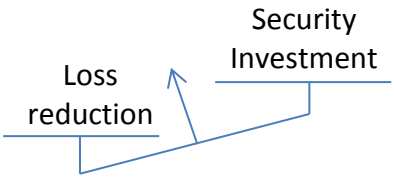
Applied to security, a Return On Security Investment (ROSI) calculation can provide quantitative answers to essential financial questions:

- Is an organization paying too much for its security?
- What financial impact on productivity could have lack of security?
- When is the security investment enough?
- Is this security product/organisation beneficial?

2.2 The false notion of *security* investment

The classical financial approach for ROI calculation is not particularly appropriate for measuring security-related initiatives: Security is not generally an investment that results in a profit. Security is more about loss prevention. In other terms, when you invest in security, you don't expect benefits; you expect to reduce the risks threatening your assets. With this

approach, the quantitative assessment the Return on Security Investment is done by calculating how much loss you avoided thanks to your investment.



The aim of cost-effective security.

3 Methodology for ROSI calculation

Assessing security investment involves evaluating how much potential loss could be saved by an investment. Therefore, the monetary value of the investment has to be compared with the monetary value of the risk reduction. This monetary value of risk can be estimated by a *quantitative risk assessment*.

3.1 Basic concepts of risk assessment

Quantitative risk assessment is achieved by determining several components of a risk. The following notions need to be defined:

Single Loss Expectancy (SLE)

The SLE is the expected amount of money that will be lost when a risk occurs. In this approach, SLE can be considered as the total cost of an incident assuming its single occurrence.

Due to the specific nature of cyber incident, the major complexity is to take into account all the assets this incident has an impact on. For instance, a stolen laptop will not only cost the replacement of the laptop itself but will also imply productivity loss, reputation loss, IT support time and, possibly, cost of intellectual property loss.

The total cost of an incident should include the cost of direct losses (website downtime, hardware replacement, data loss replacement, etc.) and the cost of indirect losses (investigation time, loss of reputation, impact on image, etc.).[2]

There are no universal values for SLEs. What will be included in the calculation of the SLE of a specific threat will depend on the business objectives, cultural values and existing security measures. In the end, one entity could estimate the SLE of a stolen laptop to the value of the laptop itself (i.e. 2.000€) while another organisation dealing with highly-sensitive information would value this loss to 100.000 € as it would affect its image, its potential contracts and its competitive advantage.

Although the SLE can be evaluated in different ways, the ROSI calculation often implies comparison of different SLEs. Therefore, it is important to be **consistent** in the way it is calculated.

Annual Rate of Occurrence (ARO)

The ARO is a measure of the *probability* that a risk occurs in a year. Again, this data is an approximation and can depend on many factors: the ARO of a flood will depend on geographic factors, the ARO of a disk failure is influenced by the operating temperature, the ARO of a burglary will depend on the location of the asset, etc. And, of course, the ARO is also

[2] *See detailed* Cost of ICT incident calculation *exercise, "CERT exercise handbook", ENISA, 2012*

depending on the existing security measures: the ARO of a successful malicious code attack will decrease significantly after implementing an effective anti-virus.

Annual Loss Expectancy (ALE)

The ALE is the annual monetary loss that can be expected from a specific risk on a specific asset. It is calculated as follow:

$$ALE = ARO * SLE$$

3.2 ROSI calculation

The ROSI calculation combines the quantitative risk assessment and the cost of implementing security counter measures for this risk. In the end, it compares the ALE with the expected loss saving.

Return on Security Investment (ROSI)

Following the ROI definition, the ROSI is defined as below:

$$ROSI = \frac{Monetary\ loss\ reduction - Cost\ of\ the\ solution}{Cost\ of\ the\ solution}$$

Implementing an effective security solution lowers the ALE: the more a solution is effective, the more reduced is the ALE. This *monetary loss reduction* can be defined by the difference of the ALE without the security solution versus the modified ALE (mALE) implementing the security solution.

$$ROSI = \frac{ALE - mALE - Cost\ of\ the\ solution}{Cost\ of\ the\ solution}$$

Which also equals to the *mitigation ratio* of the solution applied to the ALE:

$$ROSI = \frac{ALE * mitigation\ ratio - Cost\ of\ solution}{Cost\ of\ solution}$$

Example 1:

The Acme Corp. is considering investing in an anti-virus solution. Each year, Acme suffers 5 virus attacks (ARO=5). The CSO estimates that each attacks cost approximately 15.000 € in loss of data and productivity (SLE=15.000). The anti-virus solution is expected to block 80% of the attacks (Mitigation ratio=80%) and costs 25.000€ per year (License fees 15.000€ + 10.000€ for trainings, installation, maintenance etc.).

The Return on security investment for this solution is then calculated as follow:

$$ROSI = \frac{(5 * 15000) * 0.8 - 25000}{25000} = 140\%$$

According to this ROSI calculation, this anti-virus solution is a cost-effective solution.

In the end, ROSI calculation is based on 3 variables: estimated potential loss (ALE), estimated risk mitigation, and cost of the solution. If the cost of the solution is easier to predict – provided all indirect costs are considered – the two other variables are estimations that makes ROSI more approximate.

The data imperative

Imagine you calculate the cost – reputational costs, loss of customers, etc. – of having your company's name in the newspaper after an embarrassing cybersecurity event to be $20 million. Also assume that the odds are 1 in 10,000 of that happening in any one year. ALE says you should spend no more than $2,000 mitigating that risk.

So far, so good. But maybe your CFO thinks an incident would cost only $10 million. You can't argue, since we're just estimating. But he just cut your security budget in half. A vendor trying to sell you a product finds a Web analysis claiming that the odds of this happening are actually 1 in 1,000. Accept this new number, and suddenly a product costing 10 times as much is still a good investment.

It gets worse when you deal with even more rare and expensive events. Imagine you're in charge of terrorism mitigation at a chlorine plant. What's the cost to your company, in money and reputation, of a large and very deadly explosion? $100 million? $1 billion? $10 billion? And the odds: 1 in a hundred thousand, 1 in a million, 1 in 10 million? Depending on how you answer those two questions -- and any answer is really just a guess -- you can justify spending anywhere from $10 to $100,000 annually to mitigate that risk.

Source: Bruce Schneier, Security ROI, http://www.schneier.com/blog/archives/2008/09/security_roi_1.html

4 The limits of ROSI

Estimating the amount of money saved from losses that may never happen is a hard task that, in the real world, requires more than straightforward application of simple formulas.

4.1 The drawback of estimation

The ROSI calculation is the result of many approximations. The cost of cyber security incidents and annual rate of occurrence are hard to estimate and the resulting numbers can very highly from one environment to another. These approximations are often biased by our perception of the risk and the ROSI calculation can be easily manipulated (See 'The data imperative') to serve the user's interest or to justify a decision rather than enlighten it.

The accuracy of statistical data used in the ROSI calculation is therefore essential. However, actuarial data on security incidents are hard to find as companies are often reluctant to provide data on their security incidents.

Trust your experience

It's often a better practice to extrapolate from the organisation's historical data on incidents than to rely on the study of a vendor. In practical terms, if, in the past 5 years, a website has been the target of a denial-of-service attack 6 times then an ARO of 6/5 would be more accurate then a percentage related in any study.

4.2 Gordon & Loeb Model

Lawrence Gordon and Martin Loeb are economists at the University of Maryland. Their study, published in 2002, "The Economics of Information Security Investment"[3] is well known and often cited (*552 references according to Scholar Google*).

[3] *"The Economics of Information Security Investment ", Lawrence Gordon and Martin Loeb, http://ns1.geoip.clamav.net/~mfelegyhazi/courses/BMEVIHIAV15/readings/04_GordonL02economics_security_investment.pdf*

In their study, the authors state that, contrary to the basics of risk assessments, an asset of greater value should not necessarily benefit from a greater investment to protect it. The optimal information security investment does not always increase proportionately to increases in vulnerability; there is a point at which it is not in the best interest of a firm to make increasingly larger investments in information security.

According to this study, "*the optimal amount to spend on information security never exceeds 37% of the expected loss resulting from a security breach (and is typically much less that 37%). Hence, the optimal amount to spend on information security would typically be far less than even the expected loss from a security breach*".

The Gordon & Loeb model has been questioned by another study[4] showing that there was possibly no fixed percentage for optimal investment.

These conflicting studies show that ROSI calculation remains an approximate model and that the resulting numbers should be regarded with care. Organisations should consider the results as guidelines rather than strict rules to follow. ROSI calculation will never be perfectly accurate.

[4] *"On the Gordon&Loeb model for Information Security Investment", 2006, Jan Willemson, Universtity of Tartu, http://weis2006.econinfosec.org/docs/12.pdf*

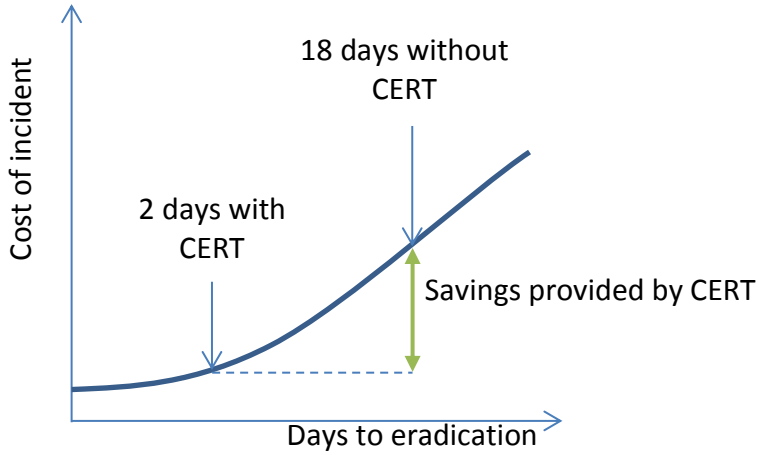
5 Assessing the cost-effectiveness of CERTs

CERTs internally providing services to an entity are "non-profit" organisations; their goal is not to make money but to prevent losses by avoiding, containing and recovering from an incident in a quick and efficient way. Therefore, the cost-effectiveness of CERTs has to be regarded as security investment: their returns on investments are the savings they provide.

A factual approach is advised here: ALE is often easier to calculate a posteriori, from more accurate historical data. Therefore, assessing the cost-effectiveness of CERTs can be approximated by assessing the difference of past incident response cost done with CERTs versus what would have been the incident response cost without CERTs.

> Cyber-attacks can get costly if not resolved quickly. Results show a positive relationship between the time to contain an attack and organisational cost. The average time to resolve a cyber-attack was 24 days, with an average cost to participating organisations of £135,744 over this 24-day period. Results show that malicious insider attacks can take more than 50 days on average to contain.
>
> *Source Ponemon Study, Oct. 2012 – Cost of cybercrime UK*
> *http://www.hpenterprisesecurity.com/collateral/report/HPESP_WP_PonemonCostofCyberCrimeStudy2012_UK.pdf*

As a rule of thumb, the quicker an incident is detected, the less expensive it is to recover from it. Depending on the type of incident, damages can grow exponentially over time. Therefore the time-saving provided by CERTs activities in incident eradication represents a financial saving in terms of damage and downtime reduction. The actual savings provided by a CERT can then be estimated by summing all the savings provided to its constituency.



CERT leads to faster response which leads to savings

Obviously, to estimate the net savings of CERT, the cost of operating a CERT has to be deduced from the overall savings. In that matter, the cost of logistics such as building, trainings, administrative, materials, etc. will have to be deduced from the savings a CERT provides and the resulting number will be the actual savings of a CERT.

6 Remaining issues and further reading

This introductory study offers a quick overview on how cost-effectiveness of security can be approached. ROSI is a complex topic and despite the numerous studies on this topic, a lot of aspects remain unresolved.

Gathering statistical data

Data accuracy is essential in ROSI calculations. Unfortunately, the threats move quickly and companies are often reluctant to reveal data on their security incidents. Therefore, little statistical information exists on the occurrence and cost of incident and effectiveness of security measure. Some CERTs regularly produce activity reports and incident statistics. These are valuable information to better estimate the Annual Loss Expectancy of a threat.

Some interesting figures:

Title	URL
ENISA annual incident report	http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2011
CSI Computer Crime and Security Survey	http://gocsi.com/survey
CSIRT CZ	https://www.csirt.cz/files/csirt/statistics/stats.html
US Department of Justice: PRO IP Act, Annual report	http://www.justice.gov/dag/iptaskforce/proipact/doj-pro-ip-rpt2011.pdf
US Bureau of Justice Statistics: Cybercrime against Businesses, 2005	http://bjs.ojp.usdoj.gov/content/pub/pdf/cb05.pdf
US Cert, 2011 Global Security Statistics and Trends	http://buildsecurityin.us-cert.gov/swa/presentations_032011/CharlesHenderson-2011GlobalSecurityStatsAndTrends.pdf
Trustwave Global Security Report	https://www.trustwave.com/global-security-report
Symantec Internet Security Threat Report	http://www.symantec.com/threatreport/
Verizon Data Breach Investigations Report	http://www.verizonbusiness.com/about/events/2012dbir/ http://public.tableausoftware.com/views/VERISCommunity/DemographicsandAgent http://www.veriscommunity.net/

Other models

The ALE model presented here is a classic approach to calculate ROSI. More complex models exist. For instance, the Net Present Value model[5] takes into consideration the decreasing value of saved income.

The Australian Department of Finance and Services introduced a hybrid ROSI calculation model combining ALE and an Australian risk assessment method called Threat and Risk Assessment (TRA). This method is based on tables covering the possible threats and their counter measures. In this bottom-up approach, each risk and its associated counter measure are evaluated resulting in a global ROSI calculation for an entity. This model is detailed in the *Guide for Government Agencies – Calculating Return on Security Investment*[6].

ROSI Calculator

Tools exist to help the calculation of ROSI. Although they can present a simplified and partial view of this complex task, they are useful to support the workflow and calculations involved in this process:

http://www.iso27001standard.com/en/rosi/return-on-security-investment

[5] *See Waldo Rocha Flores et al., Assessing Future Value of Investments in Security-Related IT Governance Control Objectives – Surveying IT Professionals, http://www.ejise.com/issue/download.html?idArticle=773*

[6] *http://www.services.nsw.gov.au/sites/default/files/ROSI%20Guideline%20SGW%20%282.2%29%20Lockstep.pdf*

7 Conclusion

This introductory paper presents the basis of Return on Security Investment calculation and how it can help CERTs in assessing their cost effectiveness. ROSI is a complex topic and this first attempt to introduce this topic has to be further developed to address remaining issues on CERTs and ROSI calculation: Which model best applies to CERTs? What to include in the cost of an incident? How to measure the added value of CERT teams in incident handling? How can CERTs estimate the value of assets they protect indirectly? How this valuable information could be shared among CERTs and benefits to all the community?

The FIRST Metrics SIG[7] is working to better the metrics and evaluation methods for internal evaluation of CERTs. As part of this work, the Metrics SIG is addressing the topic of cost of incidents and return on security investment. The results of this research will help CERTs in assessing their profitability.

[7] *See http://www.first.org/global/sigs/metrics*

8 Annex I: References

- Return on Security Investment (ROSI): A Practical Quantitative Model, no date, http://www.ra.cs.uni-tuebingen.de/lehre/uebungen/ss09/introsec/ROSI-Practical_Model.pdf,
- K. J. Soo Hoo. How much is enough? A risk management approach to computer security. http://iis-db.stanford.edu/pubs/11900/soohoo.pdf, June 2000.
- CERT podcast: Security for business leader – The ROI of security http://www.cert.org/podcast/notes/2roi.html
- Tom Campbell, SANS Institute - An Introduction to the CSIRT Set-Up and Operational Considerations, 2004, http://cyber-defense.sans.org/resources/papers/gsec/introduction-computer-security-incident-response-106281
- ISACA - IS Auditing Guideline: G41 Return on Security Investment (ROSI), 2010, http://www.isaca.org/Knowledge-Center/Standards/Documents/G41-ROSI-5Feb10.pdf
- Christian Locher, Methodologies for evaluating information security investments, 2005, http://csrc.lse.ac.uk/asp/aspecis/20050136.pdf

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu