Return on Security Investment

Alessandro Vallega
English version by Dominick Jerome Leiweke

Executive summary

- ICT security investment decisions are usually taken when companies are about to venture (1) in new digital transformation projects or (2) for reasons related to risk reduction, compliance, brand protection, or to reduce the cost of security measures.
- Calculating the economic return on security is made complex by the unavailability of required information and by the lack of adequate processes and procedures to measure it.
- Companies tend to underestimate the probability and impact of incidents and often simply invest for compliance reasons, in order to avoid breaking the law. Luckily, compliance nowadays allows investing in security measures in ways that are useful to the company.
- In this specific period, instead of calculating ROSI, it would be better to find some criteria to optimize the needed investments, to identify the areas with the most added value of security and where it is easiest to communicate the importance of security to top management.
- For some technological areas, such as information security on databases and on infrastructures of identity and access management, Oracle offers tailored programs to achieve the related specific goals.

Introduction

A main topic to understand the outlook of ICT security in Italy and in the world is tied to the understanding of corporate investment logics, the way project ROIs are evaluated, and the difficulties in connecting the security investments to such logics, or in other words, the challenge of calculating them mathematically. In most cases, security investments are treated as costs without returns, and therefore, according to regular business logics, to be avoided or reduced to the minimum. Understanding this is important for many reasons. It is important for the ICT Security responsible (the so called CISO – Chief Information Security Officer) in order for him to be able to define strategies and goals that are coherent, and therefore, sustainable and achievable; it is important for Top Management for them to overcome the limits of traditional approaches and, finally, it is important for auditors, accountants, analysts, the public and the market, who often see or suffer the nasty effects of scarce security and should act, or influence what is in their power, to change the status quo.

> *"ROSI for an enterprise is an important measure in today's cyberworld, in which hackers, computer viruses and cyberterrorists are making headlines"* – ISACA

Figure 1: Return On Security Investment[1]

In the last years we have observed a wide redesign of information systems due to the adoption of new business models or go-to-market strategies. Companies are innovating their commercial channels and making profit in new ways, taking advantage of mobile technology, social networks, big data and the cloud. We are talking about digital transformation. In such cases, the services should be secure by definition: for example, it would be unacceptable, today, to deliver an insecure Payment App. In these cases, the ROI is calculated on the total investment and the cost of security concurs solely to the definition of the total costs. Practically speaking, a ROI analysis is not conducted on the new App without security.

Therefore, the ROSI issue rises in cases in which the security investment cannot be directly associated to the digital transformation. But these cases are numerous and important. The problem is that current systems are widely unsecure, since they were created during a period of strong and hectic technological innovation in which the cyber threat was not considered real yet. Finally, looking closely, you realize that even the digital transformation does not come about from nowhere, but the new services it introduces often are delivered over current information systems and build upon them; it is generally unwise to build on uncertain grounds, but it is certainly hard to charge all the costs necessary to heal the bad quality of an entire information system on the single next digital transformation project.

Given this premise, and excluding the lucky case of digital transformation, we hereby try to dig in the logics of ROSI calculation.

When speaking of investments, the obvious problem is to calculate their return to be able to evaluate the different alternatives. You generally pick the one with the greatest and fastest economic return. One of the most commonly used formulas is that of the Return on Investment (ROI), which compares the margin with the costs required to generate it, therefore subtracting the cost from the profit and dividing the result by the cost. The entrepreneur, or the manager, can then choose between investment A and B, whether to innovate the assembly line or create a new eCommerce platform.

$$ROI = \frac{\text{Expected Return} - \text{Cost of Investment}}{\text{Cost of Investment}}$$

Figure 2: ROI formula

Unfortunately, in the specific case of ICT Security investments, it is difficult to estimate the related profit. What benefits will installing a solution of data loss prevention bring? Certainly not a positive cash flow, rather perhaps a reduction of possible damage. Here things get tricky because it is difficult to

[1] From G41 Return on Security Investment (ROSI) Effective 1st of May 2010

calculate three key factors: The value of the possible damage, the probability of incurring in the damage in case the data loss prevention solution is not installed, and the residual probability, by which we intend the chances that the damage will occur despite having installed the new technology.

In the experience of the respondent experts, in 2009 (at the time of the first Security Summit[2]), companies did not calculate the ROI on security, they did not do it in 2012 (when the first Clusit Report on Cyber Security was published) and are not doing it nowadays either. However, they all agree on the fact that it would be useful to have a method to do it, and online, or among professional associations, there are many papers and guidelines to approach the challenge. We hereby recall a publication of ours in Italian (AIEA, Clusit, Deloitte, Ernst & Young, KPMG, Oracle e PricewaterhouseCoopers – http://rosi.clusit.it), published in 2011, which carries the merit of having highlighted the main issues on ROSI and providing behavioral suggestions to the CISO[3].

Then which criteria do companies use to decide on the security investments? And is it useful to insist in trying to calculate the ROSI?

The reasons for which a company invests in ICT Security can be interpreted as a mix of the following four:

1. Reducing Risk
2. Guaranteeing Compliance
3. Protecting the Brand
4. Reducing the cost of controls

Reducing Risk

Companies invest to reduce the possibility or negative consequences of an information attack or incident, acknowledging the value for themselves and others of the assets to be preserved. Therefore, a careful investment should be preceded by risk analysis, data classification and asset inventory[4], all certainly useful activities, but which require a cultural leap and relevant investments.

The company directors who are most interested in this aspect should be the Chief Financial Officer (CFO), the Chief Risk Manager (CRM) and other C-levels with respect to their own functional area.

Some methods to calculate ROSI are based on the assumption that information incidents are numerous but do not produce big damages singularly. Therefore, these methods allow to simply multiply the

[2] Security Summit, organized by Clusit, is the most important Italian Security Conference taking place every year in different cities. https://www.securitysummit.it/

[3] "ROSI Return on Security Investments: un approccio pratico. Come ottenere Commitment sulla Security" http://rosi.clusit.it/views/Homepage.html

[4] "The First 100 Days of the Information Security Manager" http://bit.ly/100d-EN (in Italian "I primi 100 giorni del Responsabile della Sicurezza delle Informazioni"; http://100giorni.clusit.it/views/Homepage.html)

probability of an incident occurring with the damage it would cause, with and without the security investment.

Unfortunately, they are vulnerable to the manifestation of a big and unlikely negative event[5] that would produce a multimillion dollar worth damage and be able to compromise the very survival of the company[6].

Furthermore, the concept of probability is useful in relation to certain types of event, such as, for example, winning a lottery, while it presents limitations when accounted in relation to an attacker who deploys his intelligence and capabilities against our countermeasures. In this situation it is rather useful to evaluate the probability of being breached accounting for the effort the attacker invests (and skill level) and the attractiveness of the company's assets[7].

Who invests in security to reduce risk, usually does it without formally analyzing it, without classifying data nor inventorying assets, exception made for some banking institutions which are getting close to processing risk correctly. Furthermore, the tendency is to protect the portion of IT infrastructure that is exposed to Internet the most, because incidents occurring there are very visible and easier for management to understand, making it easier to raise resources for security investments. However, this leaves the company vulnerable to attacks coming from (or passing by) inside the company.

Guaranteeing Compliance

Many investments in specific security measures are the result of obligations from third parties. These can be the country through laws, local and international authorities like the one responsible for Personal Data Protection (Privacy), the European Union through the definition of regulations and directives which are locally enforced on the basis of the local context, or also economic actors who are bound by agreed upon or commercially forced rules (for example those on credit card protection). Furthermore, the obligations can be self-imposed, for example by the holding company, or as a business choice to obtain advantages, such as those tied to the achievement of an ISO certification. Limiting the considerations to the first case (external obligations), we observe two facts: the first is that usually compliance requirements tend to be drafted to protect the rights of third parties that interact with the company. This is the case of privacy laws, which define how to protect customers' personal data, or of laws that regulate access to the control systems, that insist on critical infrastructure to avoid damage to citizens,

[5] Suggested read: "The Black Swan: The impact of the Highly Improbable" by Taleb Nassim N.

[6] Many attacks presented in the Clusit Reports of the past years have cost more than 100 million euro as plain direct damage. Which Italian company can afford such costs? Furthermore, the only attacks that are publicly disclosed are generally those involving third party rights (like citizens who are stolen credit card information), while the loss of commercial secrets (like the "top clients" list) or industrial ones (like plans, projects and so on) to competitors are hardly disclosed and are therefore not published in the Clusit Reports.

[7] Thanks to Sergio Fumagalli – Zeropiù and Andrea Longhi – ConsAL for their comments and we suggest the following reading from Bruce Schneier http://bit.ly/ROSIBRUCE

or that verify the quality of a bank's credits to protect the economic system as a whole. This implies that compliance does not simply take care of the company's well being, but rather protects the subjects it interacts with, so it is normal that some very important security aspects are left to management's discretion, who has to, or at least should, take them into account (to reduce risk).

The second fact we observe is that, luckily, the formulation of compliance requirements is slowly improving thanks to a certain degree of collaboration among policy makers, through public consultations, industrial forums, interest groups and references to international best practices. Compliance requirements written in the beginning of the years 2000 included prescriptions such as: "The keyword, when required by the authentication system, is composed of at least eight characters or, in case the electronic device does not allow it, by a number of characters equal to maximum that is allowed"; while more modern ones would recite: "In designing, developing and maintaining internet payment services, PSPs [i.e. providers] should pay special attention to the adequate segregation of duties in information technology (IT) environments (e.g. the development, test and production environments) and the proper implementation of the "least privileged" principle as the basis for a sound identity and access management" [8].

These new formulations can allow a company to transform an obligation in an opportunity, with minimal extra effort, to use the same or adapted measures implemented to be compliant (third party rights) to achieve operational risk (company rights) goals. A research of PMI-NIC (Project Management Institute, Northern Italy Chapter) and Clusit, published last year and recalled in the 2014 Clusit Report, indicated that 48% of investments in IT Security[9] is realized for compliance reasons and that 47,7% is justified by risk considerations. This indicates that a lot of effort is invested in compliance and that it is worthwhile to leverage it.

Calculating compliance related ROSI might interest the Chief Executive Officer (CEO) and the Chief Compliance Manager (CCM), and should take into account the negative effects of missing compliance (economic value of issuable fines, personal effects on top managers, effects on the company both in terms of legal responsibility[10] and of public image) as well as the direct positive effects of compliance (declaring to be compliant increases stakeholders' trust towards the company and benefits its image). Obtaining a ISO 27001 certification can represent a competitive advantage and reduce the costs of internal and/or external audits.

In the past years, in Italy, numerous ICT Security investments have been guided by the laborious production of measures and guidelines, both general (for example System Administrators[11]) and

---

8 http://www.ecb.europa.eu/pub/pdf/other/recommendationsforthesecurityofinternetpaymentsen.pdf?d9d3c572d5484d0767b39d8d84c7d2c9

9 In Italy, according to the 286 certified project manager respondents. Single answer.

10 In Italy, legislative decree 231/01.

11 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1577499

industry-specific (for example FSE[12] and Banking Operations' Traceability[13]) by the Italian Data Protection Authority. In the last couple years, banks have paid a great deal of attention to the 15th update of the Circular number 263 issued by Banca d'Italia, which recites in its premise: "For this reason, banks will evaluate the opportunity of adopting international standards and best practices regarding governance, management, security and control of the information system". The financial sector will be increasingly influenced by general and specific compliance requirements in the future, which will have a relevant impact on its information systems. With respect to all other industries, the new European Privacy Regulation is on its way to be issued, which, among other important prescriptions, stresses the importance of Privacy by Design and the obligatory notification of data breaches towards the interested parties. We expect legislators and companies to tackle new compliance requirements and draft contractual rules in relation to the big themes of mobile (and mobile payments), the (public) cloud, big data, social networks and the internet of things. Compliance will influence IT investments in every industry for the coming years.

Protecting the Brand

Certain investments in security measures are made to protect the company's brand value, its fame and increase or maintain the trust of its customers and clients. Italian companies, according to our direct experience, and to the above mentioned PMI-NIC / Clusit research, are barely concerned about protecting the brand through ICT security. The relation between the two objects seems to be unclear to them. It is however likely for this to change in the near future, and this may interest both the Chief Executive Officer (CEO) and the Chief Marketing Officer (CMO), because of the effects of the European Privacy regulation we spoke about before, and because of the general increase of the companies' relational reach across the globe (induced by the adoption of eCommerce and Social / Mobile channels to attract new customers). In many industries, because of the constant reduction of margins, up-sale and cross-sale strategies are increasingly important for the company, and they depend on solid trust towards the brand. If a ROSI is calculated, it could quantify the economic value of image damage in case of an ICT security incident, considering the probability that the event becomes of public domain and estimating the reaction

1. Each of the four investment reasons presents different characteristics and problems in relation to the ROSI calculation. Collecting and defining the elements to factor in the equation is quite a challenge.

2. Every reason is of interest to a particular group of stakeholders, which complicates the approval of budget releases for such investments, especially for bigger projects, which insist on more than one budget pool.

3. The good news is that the security measures are converging, which is positive under many aspects. We can thank increasingly mature compliance policies for this.

[12] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1634116 and http://fse.clusit.it/views/Homepage.html

[13] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1813953

(more or less spontaneous[14]) of consumers and other internet players.

Reducing the cost of controls

In this last category, we include security investments aimed at reducing the cost of controls or increasing their quality and efficacy. For example, you may think about the manual production of audit reports that count all users who are enabled to access a certain group of information systems, verifying their privileges and incompatibilities in detail (segregation of duties). How much work are you willing to pay to obtain a certain quality level of controls?

In the first case, that of reducing the cost of controls, the ROSI is easy to calculate using the classic ROI definition (Figure 2: ROI); the second case is more tricky.

Evaluating the cost savings is interesting for who usually deals with budgets, such as the Chief Information Officer (CIO), the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO). This last actor is particularly interested when, as it often happens, the controls are related to the accounting and administrative functions which are subject to some compliance requirements (like when the company is listed in stock markets) and where the risk of fraud is higher. Unfortunately, in most cases, the project costs (software licenses, human labor and maintenance) outweigh the economic return, making it rare for a company to find convenience in investing for this single reason.

Final considerations on ROSI

Given the complexity of calculating ROSI, it is not easy to invest in ICT Security based on pure economic considerations, as it is often asked of Top Management. Companies that invest in security, do so because of a better understanding of what can happen without. In these years, the increasing interconnection of information systems, the blurring of the company's perimeter and consumerization have posed new security challenges for our companies to face. Unfortunately, sometimes the companies are damaged without even knowing it, like when they are subtracted secrets and intellectual property. By now, no one should believe in statements like "it's not going to happen to me", or "my data is not interesting for attackers".

Following a practical approach, instead of calculating the ROSI mathematically for each single investment, it would be better to define criteria for optimizing in the long term, to understand which areas are the most vulnerable and where to allocate security budget, which certainly has to be increased. In other words, it is useful to define criteria to allow a smart allocation of available resources in the short and the medium-long term.

It's very important to understand the need for the implementation of an organizational and technological ecosystem capable of protecting the company from attacks and incidents that can jeopardize the availability (widely recognized because of high visibility, e.g.: distributed denial of

[14] A complete model should also account for the competitors' and relevant authorities' reactions.

service), the integrity (e.g.: frauds committed through illicit use of an application) and confidentiality (harder to recognize, e.g.: data breach, theft of industrial secrets) of data, and that the measures to protect and monitor resources are to be deployed in depth, from the network perimeter, the devices, the server, the database and storage, up to the file system, operating systems and applications…

I do not believe companies act upon exclusively rational and economical reasons. The truth is that the behavior of a collective subject is the result of the interaction of many stakeholders' interests and beliefs. It is therefore necessary to keep debating about ROSI[15]: the result will be that the company can continue operating in the marketplace, being respected and keeping others from damaging the third parties it interacts with.

Security Maturity Evaluation and Oracle Insight Program

Oracle defined a method to evaluate the security of an IT infrastructure in the specific fields of databases and identity and access management. The method is based on an extensive interview, involving experts of the different professional areas within the interested company and it produces a final report with three main outcomes: illustrating the security gaps, proposing opportunities of technological and organizational enhancement and, finally, appropriately communicating to top management the importance of, and need for, implementing more controls according to the identified priorities.

About the Authors

Alessandro Vallega is Security Business Developer in Oracle WCE South; he is founder and current chairman of the Oracle Community for Security[16] and is part of the Clusit[17] Board of Directors. He defined and implemented, with colleagues, the Security Maturity Evaluation methodology.

Dominick Jerome Leiweke, Siledo Global is a young IT Consultant and Project Manager in Switzerland with a strong drive for technology and innovation. He has been part of the Oracle Community for Security for the past three years.

[15] http://bit.ly/ROSIALE

[16] http://bit.ly/oc4s_it

[17] http://www.clusit.it/index.htm