Feature

Return on Security Investment—15 Things to Consider

Ed Gelbstein, Ph.D., has worked in IT for more than 50 years and is the former director of the United Nations (UN) International Computing Centre, a service organization providing IT services around the globe to most of the organizations in the UN System. Since leaving the UN, Gelbstein has been an advisor on IT matters to the UN Board of Auditors and the French National Audit Office (Cour des Comptes) and is a faculty member of Webster University (Geneva, Switzerland). A regular speaker at international conferences covering audit, risk, governance and information security, Gelbstein is the author of several publications. His most recent book *Good Digital Hygiene—Staying Secure in Cyberspace* can be downloaded from *www.bookboon.com*. He lives in France and can be reached at *ed.gelbstein@gmail.com*.

Managers frequently request a return on security investment (ROSI) calculation. While this is a usual business practice for significant investments, the practice is not free from controversy when applied to information security.

Several guidelines and calculators are readily available, for example, the publication by the European Network and Information Security Agency (ENISA).[1, 2] As with most methodologies, they need to be applied with due care.

An information security practitioner preparing a ROSI calculation needs to prepare it in such a way to ensure that it leads to the requested resources and preserves the practitioner's credibility.

Expenditures in information security rarely, if ever, generate revenues. They may add business value in many ways, e.g., reducing the potential occurrence of a security incident, faster resolution of security incidents, supporting the organization's reputation and other essentially intangible areas.

While a marketing department faces similar challenges in justifying expenditures, it can invariably point to revenue and/or market share increases, which, like all forecasts, may or may not materialize.

The concept of value relates to the worth, importance or usefulness of something to somebody. Alas, data and information do not appear as valuable assets in balance sheets.

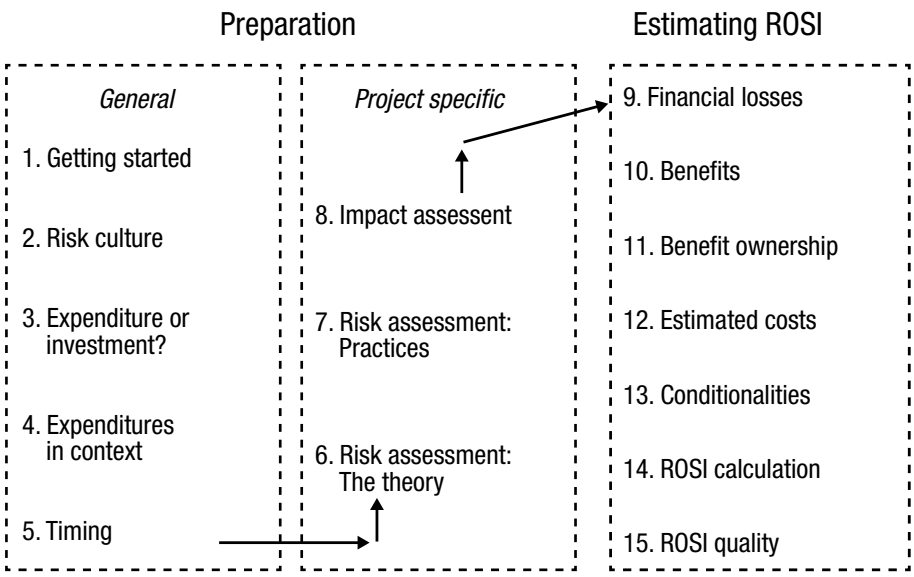
Figure 1 presents the 15 topics that practitioners need to consider in the context of their working environment to arrive at a credible and, therefore, valuable ROSI calculation.

PART I: PREPARATION

Preparation is key. Those preparing a ROSI would benefit from knowing the inventory of valuable information assets, related business impact analyses, risk analyses and their associated mitigation measures, as well as critical dependencies linked to the ROSI.

This enables the ROSI to focus on previously documented analyses, relates the proposed expenditures to them and, in this way, puts them in an appropriate business context.

Figure 1—Overview of the Steps in a ROSI Calculation



Source: Ed Gelbstein. Reprinted with permission .

The Starting Point

A ROSI calculation, however well it is done, is based on assumptions about how future security issues are likely to evolve. Likely assumptions include:

- The value of historical data on threats is low. Threats continually evolve in their nature and capabilities. Future threats may include the unimaginable.
- The impact of as-yet-identified threats is unpredictable.
- New products and processes contain unknown vulnerabilities. These may or may not be first identified by the vendor; in a worst case, hackers are the first to identify and exploit them.

The author of the ROSI needs to be aware of what assumptions have been made and be ready to explain and justify them to other managers. Good intelligence on other organizations' experiences is useful to have.

The Organization's Risk Culture

Two dominant features can be used to describe a risk culture:

- Risk appetite: conservative (risk avoidance) and aggressive (risk taking)
- Reaction towards negative outcomes: blaming and learning

Organizations with a culture of risk avoidance may go through many stages of dithering before committing to a decision, with many what-if scenarios—unless the risk is high, imminent and recognized (by which time it is no longer a risk, but an issue, and may be too late). Even then, the organization may raise questions about what options have been considered. These organizations are also likely to tend toward blame when events occur.

Risk-taking organizations may request a ROSI calculation only when large sums are involved ("large" being a flexible term).

Failure to understand the risk culture of the organization implies the possibility that the proposal will fail regardless of the quality of the ROSI. It is prudent to remember that a slice of the budget going to information security is a slice that will not go to another function, and this can become the subject of organizational politics.

The Accounting Nature of the Proposed Expenditures

The issue here is identifying what constitutes an investment and what is an operational expense. There is no universal right answer as this is defined by the accounting practices of each organization, which may be funded from different budgets, such as a revenue expenditure budget and a capital items budget, and how the budgets are treated for tax purposes.

There is also a need to distinguish between expenditures to replace or upgrade an existing facility (hardware, software and/or services) and those to acquire something new and different, as would be the case when purchasing innovative solutions, migrating to a cloud security service or outsourcing information security operations.

The argument that expenditures in information security are comparable to buying insurance or insurance-related items (e.g., better locks, fire-proof safes, inert gas fire suppression in computer rooms) may or may not be valid in any given organization. Determining the organization's thinking and practices on such topics is part of prudent preparation.

Information Security Expenditures in Context

This can be thought of as the big numbers/small numbers game. An example of big numbers can be found in the approved 2015 budget for the US Department of Defense, which identifies more than US $5 billion for cybersecurity.[3] Bigger numbers than this are in circulation elsewhere. Warning: Big numbers tend to worry decision makers and incite them to look for cuts, but small numbers can be interesting, too. A recent report by Gartner shows that in the US, the three sectors with the highest spending on information security are insurance, utilities and banking.[4] The report presents the figures as US dollars per year per employee and, assuming that there are 220 working days in a calendar year, works out at about US $2.50 per employee per day—about the price of a cup of coffee.

> "Big numbers tend to worry decision makers and incite them to look for cuts, but small numbers can be interesting, too."

A simple calculation reveals that the average total cost of an employee to an organization is in the order of US $1 per minute. Assuming that a working year consists of 220 days and that each working day is of seven and a half hours, this amounts to 99,000 minutes. The US Census for 2012 states that the median national income was US $51,371 (the highest state median income was found in Maryland [US $71,112]).[5] Adding to this all employers' costs (e.g., office space, utilities, health insurance, pension contributions), a figure of US $99,000 per employee per year appears to be a plausible estimate. Hence, US $1 per minute is a rough guide the reader may adjust to reflect specific situations.

Therefore, a person taking a cigarette break (outside the office building) of 10 minutes represents four times the amount spent on information security. (And what smoker smokes just one cigarette per day?) Are the senior managers and decision makers in the organization familiar with this perspective?

Timing Is Critical: Spend on Protection or on Correction

Software developers learned (or should have) a long time ago that the cost of getting it right the first time is much smaller than that of correcting a bug later in the development process. This, in turn, is a minute fraction of the cost of putting things right once the software is in production. Looking at design or control failures in various industries is instructive:

- Poor controls and management supervision cost the French bank Société Générale US $6.6 billion in 2008.[6] A similar situation in 2005 put Barings Bank out of business.[7]
- Airbus encountered problems with the wiring of the A380 aircraft. Redesign and delays have cost Airbus US $6.4 billion so far.[8]
- In 2014, General Motors had to recall 2.6 million automobiles to fix a defective ignition key component (valued at US $2 per unit).[9] The estimated cost so far has not yet been made public, but it is expected to be big.

It is worth remembering: Saving money regardless of cost (SMRC) is not always a winning strategy.

The Theories of Risk Assessment

There are many detailed books on the history of risk assessment[10] and, therefore, this section is deliberately short. Probabilistic theories of risk date back to the 16th and the 17th centuries and are related to games of chance. Epidemiological and actuarial theories also began in the 17th century with compilations of births and deaths in London (United Kingdom).

> "Saving money regardless of cost (SMRC) is not always a winning strategy."

By 1990, risk (and policy) analysis was seen as "an *analytical* activity undertaken in direct support of specific public- or private-sector decision makers who are faced with a decision that must be made or a problem that must be resolved."[11]

There are many definitions of "risk," each reflecting specific domains of activity, and there are several books discussing theories and their applicability as well as the languages of risk in domains such as medicine, environment, aerospace, finance and information.[12]

Risk Assessment Methods

One of the earlier probabilistic assessment techniques for the overall risk of an entire major hazard facility is considered to be WASH-1400, commissioned by the US Nuclear Regulatory Commission (NRC) in 1975.[13]

Several other quantitative methods are available, but these are believed not to be applicable to information security on the grounds that there are insufficient data, particularly on evolving threats, and that such methods are too complex. This may be the case with techniques such as Monte Carlo simulations,[14] which years ago required access to a mainframe computer and can now be carried out on almost any computer that supports spreadsheet software. However, they are not intuitive and require time to be mastered.

The belief that there are no data on probabilities is not necessarily valid. In the case of a complete lack of event intelligence (i.e., ignorance), the probability is 50 percent—either it happens or it does not. Additional information can then be used to determine if the probability is greater (it happened to someone else in a comparable line of business) or lower (it is recognized as a possible event, but it has not been reported as having happened). Such numbers may never be accurate, but are better than not having numbers at all.

There are several methods widely adopted by the information industry, notably:

- The Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE), developed by the Software Engineering Institute of Carnegie Mellon University (Pittsburgh, Pennsylvania, USA) and first published in 2001
- The US National Institute of Standards and Technology (NIST) SP 800-30 Revision 1 of 2012[15]
- *COBIT® 5 for Risk*, published by ISACA in 2013

The last one is preferred because of its historic coverage and structure and the lessons learned from the previous framework, Risk IT, which it incorporates. It may take longer to learn than drawing simple risk maps, but the result is well worth it.

Some of these methods can be criticized as being qualitative and subject to bias, therefore representing little more than an educated guess. These are also limited to known-knowns, a modest element of known-unknowns as well as not taking into account unknown-unknowns, black swans and other events thought to be extremely unlikely and, thus, rightly or wrongly treating them as irrelevant.

In an attempt to create an illusion of scientific rigor, some simple methods based on little boxes colored green, yellow or red assign weights to likelihood and impact that are then multiplied to give a number representing risk.

This can be seriously misleading. Take, for example, two ratings of five: One applies to a DVD of a movie rated by viewers as five for quality and the other to a collection of five DVDs each rated by viewers as one for quality. Does the multiplication of number of DVDs and their quality (apples and oranges) make sense?

Impact Is Multidimensional

As information systems, data and technologies are ubiquitous in most organizations, service disruption, loss of confidentiality and/or loss of data integrity are likely to have consequences beyond the IT department. The scope of impact includes direct financial losses, loss of productivity, legal implications and reputational damage from the moment a security incident is detected until it is diagnosed, dealt with, and contained, and recovery from the incident can be described as complete. There may be additional consequences, e.g., involving law enforcement, regulators, and depending on the severity of the incident and which organization suffered it, the long-term consequences of inadequate crisis management.

These should all be identified and examined by (and with) the appropriate functions in the organization. In turn, these functions should take ownership of estimates of financial losses and the benefits identified by implementing the proposed investment.

PART II: ESTIMATING THE ROSI

One may wish to choose a relevant example of a recent investment in information security and apply the following steps to acquire a better feel of what is involved and the challenges of obtaining the information required. It would be good to reflect the points raised in the previous section (part I) as part of the preparation of this exercise.

Estimating Financial Losses

Impact assessments may already be available in business impact analysis (BIA) carried out by the organization, usually to support business continuity planning. Other losses (e.g., fraud and other forms of financial theft, loss of trade secrets and other proprietary information including software) may not appear in a BIA and may be harder to predict and quantify. To these, there may be a need to add the cost of recovering data that have been corrupted.

The theft or disclosure of personal information—both customers and employees—may infringe on data protection and privacy legislation and result in disclosures and legal processes, as well as reputational loss and expenses in crisis management and public relations. Not to be forgotten, there are direct losses associated with the processes of managing a security incident through its phases of detection, containment, correction and recovery, as well as costs of invoking business continuity arrangements.

Other indirect losses may arise depending on circumstances, such as the inability to fulfill contracts, delayed deliveries, compensation payments, fines and other legal fees.

Monetizing Expected Benefits

Given that security investments, unlike those in marketing, do not generate revenue, the benefits identified are likely to include reduced financial losses (as described previously), reduced risk of a security incident occurring, reduced cost of a security incident should it happen, meeting audit and/or regulatory issues, and reduced indirect costs.

These are all forecasts to which the information security professional may not be equipped to put a financial value. It is better that they be assessed and agreed to by those who stand to gain from the benefits.

Ownership of the Benefits

To put it bluntly, any benefits listed in a ROSI calculation that do not have a clearly identified owner are not credible. Nonetheless, if presented, they risk affecting the proposer's credibility, from which it may be hard, or even impossible, to recover.

Estimating Costs

The complete life cycle of procurement includes many components that are not always included when preparing a financial case. Typically, these include the cost of preparing a request for proposals (RFP), the cost of evaluating offers, and the involvement of the procurement and legal departments in placing a contract.

Once the contract has been placed, there are the one-time costs of delivery, installation and configuration; integration with other tools when appropriate; and, possibly, training the personnel who will use whatever has been purchased.

Then, there are the recurring operating costs that include maintenance, support, upgrades and the usual data center services such as power and staff.

Conditionalities

Any purchase and installation of new facilities does not necessarily meet the buyer's requirements unless the following conditions are met:

- The product (or service) actually matches the real requirements, as these may not be quite the same as specified in the RFP.
- The product (or service) delivered works exactly as the vendor described it in its offer.
- The product (or service) is properly configured and used.

Experience suggests that these three conditions are not always met.

Calculating the ROSI

There are several formulas for doing this, from the relatively simple one proposed by ENISA to complex models involving mathematical models, differential equations and other challenges to those gifted in mathematics. Even the simple ENISA calculation contains traps for the unaware, in which the annualized loss expectancy (ALE), the mitigated ALE (mALE) and cost represent the cost of the proposed solution.

A word of warning: Before showing this calculation to finance professionals, find good answers to the following questions, which are likely to be asked:

- What does the cost include?
- What is the expected service life of the proposed purchase (amortization period)?
- How long before the benefits materialize?
- What discount factor should be used over the period?
- How long would the payback period be?

ROSI Quality

Question to the proposer: After all this effort and discussions, are your ROSI calculation and supporting documentation better than a horoscope? If so, how?

CONCLUSION

While the need for a return on investment (ROI) calculation is a well-established practice, like most activities involving predicting the future, ROSI is fraught with perils ranging from omissions (accidental or deliberate) to optimistic assumptions about costs, benefits and the effectiveness of what is proposed.

The 15 points listed may not result in a robust and credible ROSI, but showing that they have been considered and applied to the maximum possible extent may help.

ENDNOTES

[1] ENISA, *Introduction to Return on Security Investment*, December 2012

[2] The issues surrounding ROSI were explored in a previous article: Gelbstein, E.; "Quantifying Risk and Security," *ISACA Journal*, vol. 4, 2013.

[3] Corrin, A.; "Defense Budget Routes at Least $5 Billion to Cyber," *Federal Times*, 5 March 2014, *www.federaltimes.com/article/20140305/MGMT05/303050005/Defense-budget-routes-least-5B-cyber*

[4] Gartner, "Don't Be the Next Target—Information Security Spending Priorities for 2014," 8 April 2014

[5] US Census Bureau, Household Income: 2012, *www.census.gov/prod/2013pubs/acsbr12-02.pdf*

[6] Walsh, F.; D. Gow; "Société Générale Uncovers £3.7bn Fraud by Rogue Trader," *The Guardian*, 24 January 2008, *www.theguardian.com/business/2008/jan/24/creditcrunch.banking*

[7] Prof. Ted Azarmi's Forum, "Making Sense of the Collapse of Barings Bank," 25 January 2010, *www.azarmi.org/forum/index.php?topic=965.0*

[8] *http://calleam.com/WTPF/?p=4700*

[9] General Motors, GM Ignition Recall Safety Information, *www.gmignitionupdate.com/*

[10] Bernstein, P. L.; A*gainst the Gods: The Remarkable Story of Risk*, Wiley, 1998

[11] Morgan, M. G.; M. Henrion; *Uncertainty: A Guide to Dealing With Uncertainty in Quantitative Risk and Policy Analysis*, Cambridge University Press, UK, 1992

[12] For example: Rausand, M.; *Risk Assessment: Theory, Methods, and Applications*, Wiley, 2011

[13] US Nuclear Regulatory Commission, *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*, NUREG-75/014 (WASH-1400], *www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr75-014/*

[14] Microsoft Corporation, "Introduction to Monte Carlo Simulation," *http://office.microsoft.com/en-us/excel-help/introduction-to-monte-carlo-simulation-HA001111893.aspx*

[15] National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication 800-39, USA, 2011