An ounce of prevention vs. a pound of cure: how can we measure the value of IT security solutions?

Integrating a company's risk profile for threats, vulnerabilities, attacks, and outcomes to determine costs and benefits of IT security solutions

Ashish Arora[1], Dennis Hall[2], C. Ariel Pinto[1], Dwayne Ramsey[2], and Rahul Telang[1]

Introduction

According to the joint survey by the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI), information insecurities are costing companies and the overall economy millions and billions of dollars, respectively. Nowadays, the question is not whether more security is needed but how much to spend for added security. And yet investing in IT security has always been a hard-sell for IT managers. There are scores of security technologies to choose from and yet if anything is certain it is that none of them can guarantee security. Each choice involves risk. The problem is that security managers lack structured cost-benefit methods to evaluate and compare IT security solutions in light of prevailing uncertainties.

This article discusses a framework to evaluate the costs and benefits of IT security solutions using a company's risk profile. This method uses an unconventional concept of benefit based on risk avoided rather than increased productivity.

Risk-based benefit
Consider the following situation: assume virus is the only security problem and anti-virus is the only solution. The expected annual loss if unprotected is $80K. Should you then spend $80K for an anti-virus solution?

Answer: In consideration of the uncertainty behind virus attacks, it is likely that the answer is significantly less than $80K.

In this situation, the benefit is the reduced expected loss due to security failure incidents (i.e. reduction in risk). It is noteworthy that a reduction in risk does not necessarily translate to additional resources which would typically be used for other productive endeavors. In this sense, IT security activities have strong affinity with cost centers – those activities that in themselves have negative return on investment but nonetheless provide essential and necessary support for the overall organization. However, this will

[1] Carnegie Mellon University, USA
[2] Ernest Orlando Lawrence Berkeley National Laboratory, USA

not preclude the comparative and absolute evaluation of IT security solutions. Even more, the relevant criterion in evaluating IT solutions is not simply the cost of implementation but how much benefit each additional dollar of investment brings, in the form of reduced expected loss or risk.

General framework

The framework described here uses a risk management approach integrating risk profile with actual damages and implementation costs to determine costs and benefits of information security solutions. This approach requires reasonably voluminous data and thus, is well suited for organizations with extensive incident data or when consequences of incidents are high enough to warrant extensive data gathering.

Two crucial concepts are necessary. The first, *incident type*, refers to the various types of cyber incident that can happen to an organization. An incident is any undesirable event resulting from attacks against the information system. Although there is no generally accepted incident type naming scheme, most organizations track incidents on an annual basis and group them into types. Typical incident types include root compromise, malicious code (*e.g.* worms such as Slammer), and viruses, but might also include inappropriate use and spam email.

The second crucial concept is *bypass rate*. The bypass rate of a security solution is the rate at which an attack results in actual damage to the organization. It is the probability that an attack will penetrate a given security solution and result in damage to the institution. Each security solution has a bypass rate for every incident type. A 100% bypass rate means the security solution does not stop incidents of that type.

The following data are required.

1. Incident damages: This is the damage sustained by the institution in a given time period for each incident type and can be approximated by assigning an average cost per incident and multiplying by the number of incidents.
2. Implementation costs by security solution: This is the implementation and/or operating cost for each security solution. Examples of security solutions include intrusion prevention systems, firewalls, and so forth.
3. Bypass rate for each incident type-security solution pair: Bypass rates can sometimes be obtained from vendor specifications, or from white-hat type security evaluation for each security solution. They can also be approximated from interviews with the owners and operators of each security solution.

The general analysis framework has three phases:

1. Calculate the net bypass rate for all security solutions
2. Calculate total damage, incident risk and baseline scenario
3. Calculate risk-based ROI (RROI)

Figure 1 outlines the procedure and is described below:

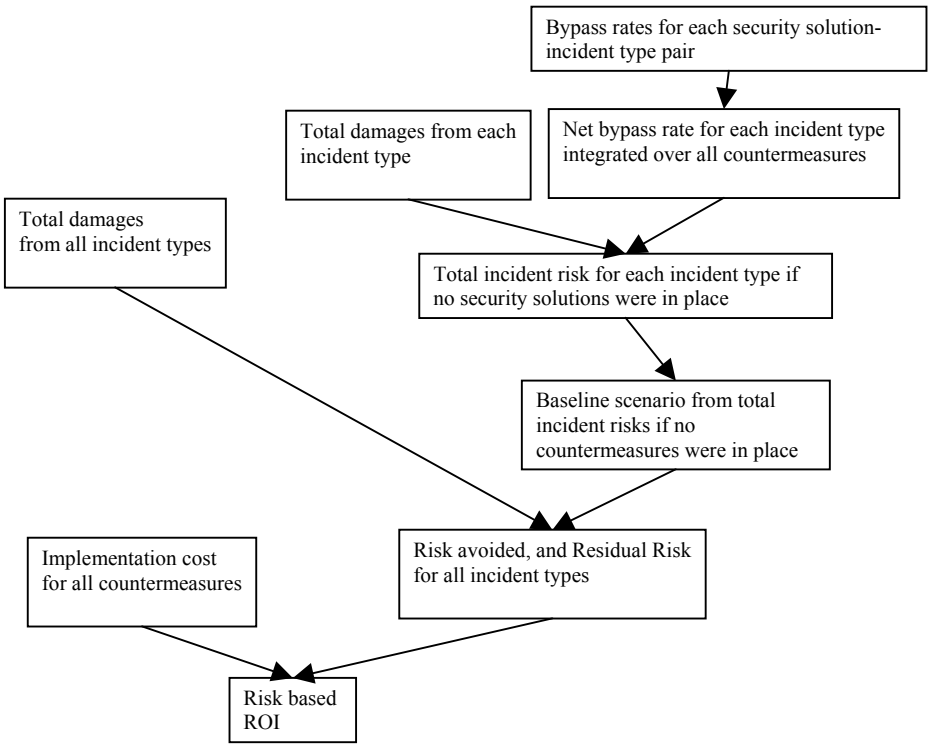

Figure 1

Calculate the net bypass rate for all security solutions
To eventually calculate the risk presented by each type of incident, the frequency of unsuccessful attacks must first be estimated. This frequency can be appraised using bypass rates, the rate at which particular types of incidents are able to pass through currently implemented IT security solutions. Determining the net bypass rate for the entire security solution requires making assumptions about how the countermeasures combine and support each other. The simplest assumption is that each countermeasure acts as an independent filter on attacks. In this case the overall bypass rate is simply the product of the individual bypass rates. The net bypass rate is calculated for each incident type.

$$\text{Net bypass rate (incident type)} = \prod \text{bypass rate (incident type, security solution)}, \quad \text{for all security solutions}$$

Calculate total damage, incident risk and baseline scenario
The damage from an incident can be derived from organizational processes and procedures that are triggered by an incident, such as root compromises or lost

productivity due to work stoppage. Also part of the incident cost are mitigation activities aimed at minimizing the damage of the incident such as scanning of servers when a virus is detected, or the reporting of security breach to an outside regulating body. Organizations that do not track cost can still estimate the damage for each incident type by estimating an average cost and multiplying this by the number of incidents. Most organizations gather data only on successful attacks mainly due to the lack of means to monitor activities outside its own network.

Actual damage describes the damages incurred even though all the security solutions are in place. If incident detection and reporting are perfect, the actual damage for each incident type is simply the reported damage for that type. Depending on the confidence one has in incident reporting, some adjustment may be necessary to compensate for unreported damages.

The incident risk is the actual damage for each incident type divided by the corresponding net bypass rate. This is the damage that would have been incurred from each incident type if no security solutions were in place:

$$\text{Incident risk (incident type)} = \frac{\text{Actual damage (incident type)}}{\text{Net bypass rate (incident type)}}$$

The baseline scenario is the grand total of all incident risks to the organization if no security solutions were in place.

$$\text{Baseline scenario} = \sum \text{Incident risks (incident type), for all incident types}$$

Residual risk is the expected value of damages if only one security solution were installed. It is calculated by multiplying each incident risk by its corresponding bypass rate for the given security solution and summing over all incident types.

$$\text{Residual risk (security solution)} = \sum \text{Incident risk (incident type)} \times \text{Bypass rate (security solution)}, \text{ for all incident types}$$

Calculate risk-based ROI (RROI)
Risk-based ROI pertains to the ratio between the net benefit in implementing an IT solution and the cost of implementation. Unlike the conventional notion where return on investment measures how effectively resources are used to generate profit, a RROI measures how effectively resources are used to avoid or reduce risk. Specifically, a positive RROI means that the degree of risk avoided is greater than the implementation cost, and a greater RROI means more risk is avoided per dollar spent in implementation.

$$\text{RROI (security solution)} = \frac{\text{Baseline risk - Residual risk - Implementation cost}}{\text{Implementation cost}}$$

In essence, a RROI is the ratio between two types of costs: the cost incurred in IT security failure incidents and the cost of thwarting these incidents. Positive RROI does not change the fact that IT security activities are primarily cost centers. As discussed in the previous section, benefit measured in terms of reduction in risk is not the same as benefit measured in terms of profit. However, the activities leading to the calculation of the RROI provide a security manager a structured cost-benefit method to evaluate and compare IT security solutions in light of prevailing uncertainties. It is important to note that RROI should be used to guide overall investment in security such that investments should be made until the RROI falls to the minimum rate acceptable to the organization.

If, however, one has to choose among *alternative* security investments, then RROI can prove misleading. *Net present value* (NPV) is the more robust and consistent alternative measure to ROI when the decision involves choosing among competing solutions. NPV considers the time value of money – the value of a dollar today versus the value of that same dollar in the future, after taking inflation and returns into account. However, the use of NPV poses a burden in requiring more detailed information such as the time when costs and benefits occur. This presents a difficult challenge in IT security solutions since the occurrence of security failure is highly unpredictable and uncertain. In fact, the high degree of uncertainty surrounding IT security incidents is what makes security investments highly difficult to manage.

Example

Suppose that an organization is evaluating several components of its IT security system in light of shrinking yearly operational budget. The objective of the evaluation is to gauge if the organization is spending too much or too little in its IT security system based on the return on investment measure. Suppose the organization has three security components already in place:

- Intrusion detection and prevention system
- Firewall
- Internal vulnerability eradication program

Furthermore, suppose incidents deemed to be the most important to the organization are the following:

- Root compromise, a hacker gaining root access to a user account
- Malicious code infections (e.g. worms and viruses)
- Improper use (i.e. leaks and potential embarrassment to the organization)

The total damage of incidents together with the bypass rates of the currently installed IT security system are used to estimate the incident risk for each incident type. Suppose that the total damage for root compromise, malicious code infections, and improper use is $5,000, $6,000, and $4,000 respectively (Table 1, row 1). Furthermore, suppose that the bypass rates for each type of incident for the components of the IT security system are established (Table 1, rows 2.1, 2.2, 2.3). Assuming that the bypass rates for the entire security system are the product of the component bypass rates, then the net bypass rates

for root compromise, malicious code, and improper use incidents are 0.225%, 0.15% and 10.0%, respectively (Table 1, row 2.4). Note that bypass rate for improper use is 100% for both firewalls and vulnerability eradication. These security solutions cannot detect improper use. However an intrusion detection and prevention system is quite effective at detecting such incidents.

The incident risk for each type of incident is the total damage divided by the net bypass rate of the entire security system. As an example, consider root compromise incidents which bypass the currently installed IT security system 0.225% of the time. The incident risk for root compromise is then \$5,000/0.225% = \$2,222,222 (Table 1, row 3 summarizes this information).

Table 1

	Types of incidents		
	Root compromise	Malicious code	Improper use
1. Total damage	\$5,000	\$6,000	\$4,000
Bypass rates			
2.1 Intrusion detection & prevention	10%	10%	10%
2.2 Firewall	15%	15%	100%
2.3 Vulnerability eradication	15%	10%	100%
2.4 Net bypass rate	0.225%	0.15%	10%
3. Incident risk	\$2,222,222	\$4,000,000	\$40,000

To calculate the risk-based ROI (RROI), the reduction in risk for each IT solution is calculated. First, consider the risk if no IT solution is implemented. This is the baseline scenario described above. The risk for such a scenario is simply the sum of the incident risks, \$2,222,222 + \$4,000,000 + \$40,000 = \$6,262,222 (Table 2, row 1).
Residual risk is the expected value of damages if only one security solution was installed. Consider the Intrusion detection and prevention solution. Its residual risk is the sum of the individual incident multiplied by their respective bypass rates. For this solution the residual risk is \$2,222,222*10%+\$4,000,000*10%+\$40,000*10%=\$626,222. This is shown in Table 2, row 2.1 along with the implementation cost of \$300,000. Residual risk and implementation costs for the other security controls are show in Table 2 rows 2.2 and 2.3.

The net benefit for intrusion detection and prevention is the reduction in risk compared to baseline scenario, less the implementation cost, \$6,262,222 -\$626,222 -\$300,000 = \$5,336,000. The risk-based ROI is then \$5,336,000/\$300,000 = 33 (see Table 2, row 2.1).

Table 2

	Residual risk	Implementation cost	RROI
1. Baseline scenario	\$6,262,222	\$0	--
2.1 Intrusion detection & prevention	\$626,222	\$300,000	33
2.2 Firewall	\$973,333	\$75,000	24
2.3 Vulnerability eradication	\$773,333	\$200,000	56
2.4 Entire security system	\$15,000	\$575,000	11

It was mentioned earlier that RROI differs from its conventional counterpart in the way benefits are viewed. In this particular example, vulnerability eradication has the highest RROI among the component solutions. An RROI of 56 means that every dollar invested in this particular component of the IT security solution yields a net reduction in risk of $56. It is timely to reiterate the appropriateness of RROI in decisions regarding how much to invest and *not* so much in choosing among alternatives, as discussed in the previous section. Suppose that the organization would like to invest as much as possible until every dollar of investment returns at least ten dollars in reduction in risk (i.e. minimum acceptable rate is 10). It is then clear that implementing the entire security system is the appropriate investment scheme since the RROI of 11 for the entire security system is above the minimum acceptable rate.

However, the decision process to manage the dilemma of choosing among security components is beyond the scope of this article. This is a case in point where sensible CISO or CIO will use more than one criterion to evaluate IT security solutions.

Challenges to applying the framework

There are two general challenges in evaluating IT security solutions: (a) complexity of integrating information on threats, vulnerabilities, attacks, and outcomes, and (b) determining the costs and benefits needed in the analysis. For the framework discussed above, particular challenges are:

Obtaining true costs
Non-cash but otherwise very relevant costs such as lost productivity and opportunity cost of security incidents are often miscalculated primarily due to difficulty in quantifying the actual amount or simply due to lack of enough information. This is particularly true in the valuation of loss of confidentiality and integrity in IT security breaches. The inherent nature of confidentiality prevents establishing the consequences of security failure, even less putting value on such consequences. However, it is noteworthy that such a challenge also occurs in other settings like physical, health, and environmental risk assessment where human lives are at stake.

The implementation cost of the solutions can also be difficult to estimate since many resources, both human and machine, are shared by several solutions during implementation. Double-counting of some costs can also result from vague definitions used in accounting and operation processes. For example, cost due to lost productivity may be difficult to differentiate from cost due to lost revenue. An operations manager may account for work stoppage due to virus attacks as lost productivity, at the same time a financial officer may account for decrease in sales due to the same instance as lost revenue, resulting to possible double-counting.

Estimating bypass rates
The bypass rate, both for existing security system and for the solutions being evaluated can be difficult to estimate due to minimal or non-existent information. Currently, the most reliable sources of this information are intrusion detection experts that have worked closely with the particular solution and have detailed knowledge of the current security system. This is especially true in evaluating new solutions where no actual performance data exist yet that suitably describe details of the existing system's architecture. More recently, there have been developments in using honeypots to directly measure potential frequency of incidents on certain types of networks without using bypass rates. However, bypass rates would still be necessary for calculating residual risk of particular solutions.

Compensating for interaction among solutions
In the example application of the framework described above, the combined effectiveness of the solutions is assumed to be multiplicative, as demonstrated by the calculation of the system-wide bypass rates. However, this simplification may not accurately describe the actual interaction of various solutions implemented concurrently. The architecture of the network and the configuration of particular solutions can result to interaction that may be too complicated to assess.

Representing catastrophic losses
A constant challenge in risk assessment is the proper representation of catastrophic incidents. In the example application of the framework, it is implied that estimates of costs, consequences, and frequencies are averages or expected values. In this process of averaging out rare but catastrophic events with frequent but inconsequential events, disastrous consequences have the potential to be neglected in the analysis. Though there are tools that deal with this type of events, their demand for detailed information or oversimplifying assumptions often preclude their application in IT security analysis.

Conclusion

There continues to be challenges in reliably estimating the costs and benefits of IT security solutions that go beyond the coverage of the framework presented in this article. Changing technologies, both on the attack and defense fronts of IT security, and evolving network architecture can result in the continuous influx of new and untested security solutions. Prevailing economic climate also increases the demand for CIO's and CISO's to be more prudent in investing on IT security solutions. Together, these forces make structured cost-benefit methods evermore vital in evaluating and comparing IT security solutions. However, for these same two reasons, uncertainties surrounding the current and future states of IT security continue to hinder reliable analysis of available solutions.

On the other hand, current trends support the basic activities of this risk-based framework. Industry consortiums such as the Cylab (http://www.cylab.cmu.edu/), and the Sustainable Computing Consortium (http://www.sustainablecomputing.org/), federally funded entities such as CERT/CC (http://www.cert.org/), and independent organizations such as The Honeynet Project (http://project.honeynet.org/) all continue to gather and

provide updated and more reliable information on IT security threats, vulnerabilities, attacks, and outcomes.

Since some of the methodological challenges exposed by the framework are not unique to the IT fields, efforts in the academic and research arena to develop tools and techniques appropriate for analyzing sparse or otherwise disparate empirical data typical of IT security incidents can be harnessed. These efforts are scattered in many fields such as medical testing, environmental protection, and even protection against terrorism.

Overall, IT professionals are getting a better grasp of managing security investment, and need to continue exploring unconventional avenues such as risk management in addressing IT security.

Resources

These articles cover key topics in the evolving discussion of measuring the costs and benefits of IT security solutions.

"The New Meaning of Quality in the Information Age" C.K. Prahalad and M.S. Krishnan, Harvard Business Review, September-October 1999, p. 109-118.

"Information Security: Why the Future Belongs to the Quants" D. Greer, Jr., K. S. Hoo, and A. Jaquith, IEEE Security & Privacy Magazine, July-Aug. 2003 p. 24-32.

"Is Return on Security Investment (ROSI) Impossible?" Sygate, Inc., China, 2002; http://china.sygate.com.

"Finally, a Return on Security Spending" S. Berinato, CIO Magazine, 2002; http://www.cio.com.

"Calculating Security ROI is Tricky Business" M.J. Wilson, Computerworld, Inc., 2003; http://www.computerworld.com.

Acknowledgement

This article draws extensively on a risk assessment technique developed at Earnest Orlando Lawrence Berkeley National Laboratory beginning in September 2000. Dennis Hall led the self-assessment effort and developed the technique for ranking security operations based on a quasi return-on-investment metric. Data collection and analysis was performed in collaboration with Jim Rothfuss, the Laboratory's Cyber Protection Program manager, and Dwayne Ramsey, the Laboratory's liaison to the Department of Energy.

This technique established to Laboratory management and Department of Energy auditors that it is significantly less expensive to accept some damage from cyber attacks

than to prevent all damages. This pragmatic approach enables Laboratory cyber-security staff to optimize security countermeasure investments and reduce spending without sacrificing protection.

This work was supported by the Director, Office of Science, Safeguards and Security-Science, U.S. Department of Energy under Contract No. DE-AC03-76SF00098. DE-AC03-76SF00098