Driving Value From Information Security: A Governance Perspective

Vishnu Kanhere, Ph.D., CISA, CISM, AICWA, CFE, FCA, is an expert in software valuation, IS security and IS audit. A renowned faculty member at several management institutes, government academies and corporate training programs, Kanhere is a member of the Sectional Committee LTD 17 on Information Security and Biometrics of the Bureau of Indian Standards. He is currently newsletter editor and academic relations, standards and research coordinator of the ISACA Mumbai Chapter; member of the ISACA Publications Committee; honorary secretary of the Computer Society of India, Mumbai Chapter; convener of a special interest group on security; chairman of WIRC of eISA; and convener of the security committee of the IT cell of Indian Merchants’ Chamber. He can be contacted at vkanhere@vsnl.com or vishnukanhere@yahoo.com.

With the increasing dependence of the corporate world and governments on information systems and technology, the need, importance and relevance of information security governance is well acknowledged and accepted by top management. The questions that still plague organizations at all levels are not whether, why or what to secure; the business policies and risk management framework provide the answers to these questions. Questions of when, how, to what extent and at what cost to secure business and its information systems remain.

Communicating to and convincing the board about nebulous and technical concepts and matters such as information systems and IT security have always been a challenge. The board of directors always prefers bullet points, an executive summary backed by evidence, ideally with supporting financials to help them make quick, effective and correct decisions. These decisions are ultimately made at the board level as part of the governance function.

In the present scenario, those in charge of governance generally expect proposals backed by return on investments (ROI), return on capital employed (ROCE), return on security investment (ROSI), cost-benefit analyses and balanced scorecard (BSC) workings. This article focuses on ways of putting forward a business case for information security and describes the best approach to achieve it.

INFORMATION SECURITY GOVERNANCE

Corporate governance has many dimensions: transparency, accountability, stakeholders’ interests, ethics and fair play, to name a few. It also has many subsets: governance cutting across functional areas of management, marketing, operations, logistics, finance and accounting, supply chain management, and human resource management. Information technology, a fascinating addition to the asset portfolio of a business, is also a part of the subsets to be governed. Hence, IT governance in business is an important feature. However, given the prowess of IT, protecting information system assets (i.e., hardware, software, data) and securing the intangible and tangible assets at all times are predominant desiderata of a corporate information security governance policy. Thus, a new dimension to corporate investment decision making is information security investments.

In time, IS security investment may become a mandatory proposition, not merely to protect businesses against assaults, but to protect the sovereignty and territorial integrity of a country or the world.

Admittedly, in the post 11 September 2001 scenario in the US, reinforced again by repeated terrorist attacks elsewhere, a properly implemented information security management system (ISMS) can make a vital difference to the very existence of any business. With stringent legislation in place requiring companies to secure and protect data and information assets, and the introduction of legislation such as Law 1386 in California (USA) and elsewhere, expenditure on information security is no longer a luxury or an exercise in futility, but has become a pressing need even for the small and medium-sized business.

ISSUES CONCERNING ISMS

The important questions posed before contemporary management are:

- What is the IS security investment and what are its components?
- What are the expected payoffs from the investments—proactive and reactive?
- What are the measures of performance that can be used—ROI, ROCE, ROSI and cost-benefit analysis?

Each of these issues will be discussed in turn.

What Is the IS Security Investment and What Are Its Components?

IS security investment includes, *inter alia*, inputs required to protect the IT prowess of
business from abuse by delinquents—insiders and outsiders. Thus, security arrangements include investments in people, processes to mind and manage the IT portfolio, data, information, other processes, products, people, other assets and reputation. Security arrangements require outlays on revenue and capital accounts to preempt assaults of any type on the IT prowess of business. Such a watch on IT prowess has to be a 24/7 proposition.

IT security investments must touch all echelons of IT prowess, including the smallest possible corner or cavity of the IS configuration of business.

What Are the Expected Payoffs From the Investments—Proactive and Reactive?
The payoff from any investment is usually evaluated in terms of typical profitability; time-adjusted measures of performance, including ROI; net present value (NPV); internal rate of return (IRR); and other related tools and techniques. In typical security-motivated investments, the expected payoffs are certainly not in revenues or even reduction in costs. However, the least-cost option, in terms of time, money and effort required to put a security system in place, is one technique that can be effectively used. Yet another way of looking at the evaluation of security investment is “fear” on the part of the delinquent—“big brother is watching and we may be caught.” The deterrence generated by the security solution vs. the greed that exists, either of bonanza, monetary gains or satisfaction that the destruction is done, does not matter. The greatest reward or payoff is the likelihood that more and more people will refrain from tampering with IT investments and information systems. The concomitant discipline, single-minded attention to work on the part of internal potential delinquents and the smooth conduct of operations that are compliant with the laws of the land are all potential gains, not fully quantifiable, yet very relevant. Thus, while the denominator of the ROI (investments) can be quantified, the numerator is not bereft of gains that can be effectively articulated, felt and experienced, but not necessarily quantified. However, the historic data relating to losses arising out of delinquencies can be a useful base that is amenable to measurement. If the current losses due to assaults on IT are reduced, the year-on-year reduction in IT losses is a quantifiable piece of information. The fact that IT assets and prowess thereof are protected, and that there are no, or minimal, assaults on IT assets and no loss of life, due to terror-driven infiltration, would bear testimony to the viability and raison d’etre of the security investments.

What are the Measures of Performance That Can Be Used—ROI, ROCE, ROSI and Cost-benefit Analysis?
Decision makers ask themselves: “Which of these options gives me the most value for my money?” That’s the fundamental question that ROI is designed to answer. ROI is frequently used to compare alternative investment strategies. For example, a company might use ROI as a factor when deciding whether to invest in developing a new technology or extending the capabilities of their existing technology.

\[
ROI = \frac{\text{Expected Returns} - \text{Cost of Investments}}{\text{Cost of Investments}}
\]

To calculate ROI, the cost of a purchase is weighed against the expected returns over the life of the item. For example, if a new security project will cost US $1 million and is expected to reduce damages valued at US $5 million over the course of three years, the ROI for the three-year period is 400 percent (the net damages avoided being four times the initial investment).

A simple equation for calculating ROSI is as follows:

\[
\text{ROSI} = \frac{(\text{Risk Exposure} \times \% \text{ Risk Mitigated}) - \text{Solution Cost}}{\text{Solution Cost}}
\]

Thus, repeatable and consistent metrics can be extremely valuable—even if they are “inaccurate.”

A simple analytical method of calculating risk exposure is to multiply the projected cost of a security incident (single loss exposure [SLE]) with its estimated annual rate of occurrence (ARO). The resulting figure is called the annual loss exposure (ALE). While there are no standard methods for estimating SLE or ARO, there are actuarial tables that give average statistical values based on actual damage reports. These tables are created from insurance claim data, academic research or independent surveys.

\[
\text{Risk Exposure} = \text{ALE} = \text{SLE} \times \text{ARO}
\]
With a good survey and scoring system for productivity, combined with external measurement of intellectual property value, it becomes possible to quantify risk exposure in a repeatable and consistent manner. Unfortunately, there are a number of serious problems with this “logic”:

• Risks cannot be captured in silos—A properly secured and locked door may fail to mitigate risks if the window next to it is open.
• Security solutions are not stand-alone—The existence and effectiveness of a framework of policies, practices, procedures and other solutions are necessary for security to be viable.
• Security solutions are rarely implemented to be as effective as possible due to an unacceptable impact on productivity.
• Security solutions become less effective over time, as hackers find ways to work around them and create new risks.

A CASE STUDY
Security programs strive to control and minimize loss by preventing undesirable things from happening or mitigating the impact and its effects when they do occur. Consequently, determining the efficacy of a security program and quantifying ROSI is difficult because it requires measuring something that has been prevented: losses that were avoided. Measuring something that has been avoided is extremely challenging and may be impossible in many situations.

A leading computer chip/computer manufacturer developed a model for measuring ROSI in its manufacturing environments that produced a much higher level of accuracy than other methods currently being used. The model has enabled it to make business-driven decisions about security programs, resulting in savings in excess of US $18 million per year in avoided losses. By analyzing historical cyberattack incidents, performing trend analysis of data from similar environments and then extrapolating, the model is able to predict interim trends in security incident occurrence to derive the financial impact of technology adoption for security programs.

This ROSI methodology is scalable, manageable and can be automated, providing managers with an effective tool for calculating value, making decisions, justifying outlays on information security, allocating resources and implementing an optimal level of security. The data set included incident data, such as virus and worm events, tracked for two years, and information from approximately 18,000 computers over the course of 750 days (equivalent to 13 million computer days).

Because the predictions are based on actual incident data rather than an assessment of potential exposure and vulnerabilities, the ROSI approach used by the manufacturer provides a high level of accuracy. This also enables management to compare the value of security programs with nonsecurity initiatives so that the organization is better able to manage and allocate resources, justify security expenditures, predict the value of future security programs, and determine if it is meeting expectations once implemented. This, in the long term, helps to provide the critical data necessary for developing a strategic plan for securing the computing environment.

CONCLUSION
The primary take-home is a structured methodology to budget for IT security based on the previously mentioned approach. Certain key issues to be considered are:

1. Business cases differing from the view of law enforcement and regulatory and government agencies, e.g., settlements of credit card fraud cases
2. Security as a trade-off among cost, convenience and computing performance in terms of flexibility, speed and performance
3. Retrofitting security vs. designing a new system for information security
4. Balancing limited funds, unlimited choices and too many viewpoints
5. Protecting the right things. Think like the hacker, keep the bad guys out, but let the good guys in (in all of these, “good” and “bad,” “right” and “wrong,” are relative terms).
6. Regulatory compliance. One size does not fit all. A bank, a military installation, a manufacturing company, an ISP, a web site, a small business—will all of them react in the same way?
7. Cost of gold plating, bells and whistles in IT security
8. The appropriate level of security, depending on who, where, why, what and how information is protected
9. Experience—perhaps the most expensive, but the most effective teacher. Insecure computers cost time, money and, in some cases, reputation and goodwill, which are much more difficult to replace when lost.
Determining the ROSI of information security projects helps in crystallizing the intangible benefits and nonquantifiable considerations. This enables management to weigh all the factors in the right perspective and to arrive at informed decisions, rather than relying on instinct alone. However, given the problems associated with information security in terms of its implementation and effectiveness, especially the dilemma of security vs. openness, conventional ROI/ROSI alone is not an appropriate tool for deciding whether to proceed with information security projects. Rather, this decision should be made on a business-case basis. ROSI would be more appropriate for making a choice between different alternatives of security investment. Hence, ROI should be tempered with an assessment of the competitive advantage of information security proposals. A balanced scorecard approach coupled with ROSI would be a better alternative (see figure 1).

Costs/benefits of IT security projects largely depend on the human factor, cost and revenue drivers, business objectives, security metrics, and organizational characteristics, which can substantially influence end results. Refining ROSI estimates through learning experience and by comparing estimated and realized ROSI will improve this tool with each successive project, resulting in better calibration and more accurate estimates. Thus, ROSI, with a balanced scorecard focus, will become a tool of choice for the future, in the hands of decision makers.

Figure 1—The Balanced Scorecard Framework Using ROSI

REFERENCES
EE Times of India, “APAC SMBs Up IT Security Investment by 26%,” www.eetindia.co.in
Surmacz, Jon; “An Ounce of Prevention—Why ROI Is the Wrong Question to Ask About Security,” CSO Online, 8 May 2002
“Finally, a Real Return on Security Spending,” CIO Magazine, 15 February 2002
Kanhere V. S. Kanhere; A. Agarwal; “Budgeting for Information Security an ROI Approach,” InfoSec, 2004