Models for Assessing the Cost and Value of Software Assurance

Antonio Drommi
Dan Shoemaker
Jeff Ingalsbe
John Bailey
Nancy Mead

February 2007

ABSTRACT: It is not enough to simply estimate the cost of doing secure software assurance: you must also justify it from a value perspective. This paper presents IT valuation models that represent the most commonly accepted approaches to the valuation of IT and IT processes. These models can be categorized into four initial types: investment based, cost based, environmental/contextual, and quantitative estimation. However, the general conclusion is that there are only two valid ways to approach valuation of the secure software assurance process: quantitative and environmental.

INTRODUCTION: ASSIGNING TANGIBLE VALUE TO A THEORETICAL PAYOFF

The commonly accepted definition of software assurance is "a level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its life cycle and that the software functions in the intended manner" [CNSS 2006].

Software assurance is a national security priority [PITAC 1999]. That is due to the common-sense fact that a computer-enabled national infrastructure is going to be as reliable as the code that underlies it [Dynes 2006, PITAC 1999]. Thus, it is easy to assume that any set of activities that increase the general level of confidence in the security and reliability of our software should be on the top of everybody's wish list.

Unfortunately, if the software assurance process is working right, the main benefit is that absolutely nothing happens [Anderson 2001, Kitchenham 1996]. And, in a world of razor-thin margins, a set of activities that drive up corporate cost without any directly identifiable return is a tough sell, no matter how seemingly practicable the principle might be [Anderson 2001, Ozment 2006, Park 2006].

The business case for software assurance is therefore contingent on finding a suitable method for valuation—one that allows managers to understand the implications of an indirect benefit such as assurance and then make "intelligent" decisions about the most feasible level of resources to commit [Anderson 2001, McGibbon 1999].

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

Phone: 412-268-5800
Toll-free: 1-888-201-4479

www.sei.cmu.edu

Several general models for assessing the value of an IT investment already exist [Cavusoglu 2006, Mahmood 2004, Brynjolfsson 2003, Mayor 2002]. It is our belief that the factors underlying these models can be used to build a business case for deciding how much investment can be justified for any given assurance situation [Cavusoglu 2006].

The purpose of this paper is to summarize the concepts and principles promoted in these models and provide a brief discussion of their common features. Below, we present the 13 most commonly cited models for IT valuation. We gleaned this list through an exhaustive review of the published ideas concerning IT valuation. Although this set is generally comprehensive, it does not encompass every approach, since several models are strictly proprietary. However, based on our review, we believe that generic models for valuation can be factored into four categories:

- Investment-Oriented Models
- Cost-Oriented Models
- Environmental/Contextual-Oriented Models
- Quantitative Estimation Models

INVESTMENT-ORIENTED MODELS

Total Value of Opportunity (TVO) – Gartner

TVO is a standard metrics-based approach invented by Gartner. Its aim is to judge the potential performance of a given IT investment over time. It centers on assessing risks and then quantifying the flexibility that a given option provides for dealing with each risk. (Gartner defines flexibility as the ability to create business value out of a particular option.) TVO is built around the four factors described below [Apfel 2003]:

- cost/benefit analysis
- future uncertainty
- organization diagnostics
- best practice in measurement

Cost/benefit analysis - Total cost of ownership (TCO) is always used to characterize the overall cost of operation. Benefits are then judged using a broad range of organizational performance measures. The recommended mechanism for benefits analysis is Gartner's Business Performance Framework [Apfel 2003]. The cost/benefit analysis must be comprehensive and appropriate to the situation, and

it must describe the business case in terms that a non-IT executive can understand [Apfel 2003].

Future uncertainty - Because IT investment rarely produces immediate benefits, TVO also requires the business to quantify any probable future impacts of a given investment [Apfel 2003]. This aspect is particularly attractive in the case of software assurance, because much of the investment in securing software is designed to ensure future advantage by preventing undesirable events. These benefits should be quantified based on assumptions that can be validated retrospectively or on data-based prospective estimates such as trend line analysis [Mahmood 2004].

Organization diagnostics - These are the heart of the TVO approach. Any alteration in practice implies some form of substantive change, and organizational diagnostics essentially test an organization's ability to adapt to that change. The three types of risks associated with change—business, management, and technology—are assessed on five factors [Apfel 2003]: Strategic Alignment, Risk, Direct Payback, Architecture and Business Process Impact. Those factors coincidentally happen to be Gartner's Five Pillars of Dynamic Benefits Realization.

Best practice in measurement - This factor simply requires the employment of a commonly accepted methodology to obtain the value estimates that underlie the Future Uncertainty factor [Apfel 2003]. The aim of the measurement process is to enable a conventional business analysis that is capable of communicating the value proposition to a general audience. The key to this part of the approach is a small set of agreed-upon business metrics. The use of common metrics ensures understanding between major stakeholders. Consequently, the development of those metrics is critical to the process.

Total Economic Impact (TEI) – Forrester

Like TVO, TEI is meant to integrate risk and flexibility into a model that will support intelligent decisions about IT investment. TEI is a proprietary methodology of the Giga Group that allows an organization to factor intangible benefits into the equation by assessing three key areas of organizational functioning [Wang 2006]:

- flexibility
- cost
- benefits

Flexibility - Flexibility is a function of the value of the options the investment might provide. It can be described in terms of enhanced financial value or increased communication potential or on the basis of potential future increases in

business value [Wang 2006]. TEI quantifies these factors using another more explicit methodology, such as Real Options Valuation (ROV) (described later in this paper). The supporting methodology can describe the actual value of the options that are available at the decision point, or it can describe the value of an option to be exercised later (for instance, an assumption that the future market share will increase as a result of an increase in assurance).

Cost - The cost analysis takes a TCO-like approach in that it considers ongoing operating costs along with any initial capital outlay. It factors both IT budget expenditures and the allocated cost of the overall organization control structure into the assessment. (The latter enforces IT accountability.)

Benefits - Benefits are expressed strictly in terms of increased business value. That expression includes any value that can be identified within the IT function as well as any value that is generated outside of IT. Thus, benefit assessments also look at the project's business value and strategic contribution and consider how appropriately the investment aligns with business unit goals.

Once these factors are quantified, the organization seeks to determine the risks associated with each of them [Wang 2006]. The risk assessment is expressed as an uncertainty or likelihood estimate that includes the potential economic impact of all major assumptions. In essence, the decision maker must be able to express both the consequences of all assumptions as well as their probability of occurrence in quantitative terms. A statement of the level of confidence in the accuracy of the overall estimate should also be provided [Wang 2006].

TEI is one of the softer kinds of value estimation methodologies and seems to be most useful when an organization's aim is to align a technology investment with a business goal or to communicate the overall value proposition of an initiative. TEI's primary purpose is to underwrite sound business decisions, given a set of alternatives [Mayor 2002]. It does that by communicating each alternative's full value in business terms. Thus, TEI can be used to justify and relate a proposed direction to any other possible directions. That creates a portfolio view of the entire IT function, which enables good strategic management practice. Since understanding the overall impacts is obviously one of the primary goals of any software assurance valuation process, TEI is an attractive approach.

Rapid Economic Justification (REJ) – Microsoft

In order for it to be acceptable, the cost of the software assurance process has to be justifiable in hard economic terms. But more important, that estimated cost must be available when needed. The problem is that most valuation techniques require long periods of data collection in order to produce valid results [Microsoft 2005].

The aim of Microsoft's REJ is to provide a quick and pragmatic look at the value of the investment, without taking the usual lengthy period of time to collect all the necessary operational data [Microsoft 2005]. Like the Total Economic Impact approach, REJ seeks to flesh out traditional TCO perspectives by aligning IT expenditures with business priorities [Microsoft 2005].

REJ focuses on balancing the economic performance of an IT investment against the resources and capital required to establish and operate it. The focus of that inquiry is on justifying business improvement [Konary 2005]. Thus, REJ involves tailoring a business assessment roadmap that identifies a project's key stakeholders, critical success factors, and key performance indicators [Konary 2005]. The latter category comprises only those indicators needed to characterize business value. The REJ process follows these five steps [Microsoft 2005, Konary 2005]:

Step One: Understand the Business Value. The aim of this step is to create an explicit map of the proposition so that both IT and business participants have a common perspective on the implications of each potential investment. That activity is proprietary to the REJ process and involves the use of a Business Assessment Roadmap that itemizes

- key stakeholders
- their critical success factors (CSFs)
- the strategy to achieve business goals
- the key performance indicators (KPIs) that will be used to judge success

Step Two: Understand the Solution. In this step, the analyst works with the owners of key business processes to define ways of applying the technology to ensure a precise alignment with the organization's CSFs. This analysis is always done in great detail, since the aim is to specify an exact solution.

As with the other models, the benefit calculation goes well beyond TCO. The analyst uses the business's commonly accepted practices to characterize process flows [Konary 2005]. The cost of each process is described from the initial planning outlay, to implementation and maintenance costs, to long-term operating expenses. The aim is to describe the investment in terms of its overall life-cycle cost and then profile that cost against all the potential benefits that might be accrued during that time [Konary 2005]. Then, REJ provides an exact quantification of the solution's value in hard financial terms [Microsoft 2005].

Step Three: Understand the Improvements. The unique feature of REJ is that it allows the organization to look beyond the traditional areas that IT might influence in order to ascertain that all potential business tasks, functions, and process-

es that might be improved by the prospective investment have been identified and characterized. This analysis must cross over all the functional areas and consider the potential benefits to both the IT function and those functions outside of IT, such as inventory, sales, and marketing [Microsoft 2005, Konary 2005].

Step Four: Understand the Risks. This step requires an accurate profile of all the potential risks, including their likelihood and impact. The key for this step is to factor the risk mitigation solution into the benefit and cost estimates [Konary 2005]. Doing so lets the organization optimize the economic impact of the step they are planning to take. A variant on this is to factor cost into a risk-based model, and use the risk model to prioritize software assurance strategies [Feather 2001].

Step Five: Understand the Financial Metrics. Finally, all aspects of the proposed investment are characterized on a conventional financial basis, such as Net Present Value. REJ aims at building a bridge between IT and business executives [Microsoft 2005]. Thus, the terminology used to communicate the business value must ensure that all stakeholders (business and IT) can be committed to both the process and the results [Konary 2005].

COST-ORIENTED MODELS

Economic Value Added (EVA) - Stern Stewart & Co

EVA approaches IT investment as a value proposition rather than as a cost. That is, EVA attempts to describe all the ways a prospective investment might leverage organizational effectiveness [McClure 2003]. EVA approaches this question by looking at a function in terms of the cost saving it might create when compared to the cost of obtaining the same function through external providers at a market rate (e.g., the cost if the service were provided by an outside vendor) [McClure 2003, Mayor 2002]. Once the comparative market value is determined, EVA quantifies the difference between the market price and the actual cost of providing the prospective function. That difference is the net operating benefit [Pettit 2001].

Costs are characterized by such things as capital outlay and opportunity cost (i.e., the potential cost of NOT doing something else). The aim of an EVA comparison is to determine whether the market value of any investment, after the actual costs are deducted, is positive [Pettit 2001]. Therefore, EVA requires a careful accounting of all expenditures as well as an honest estimate of any opportunity cost [McClure 2003].

An EVA analysis demands that everything from initial cash outlays to maintenance and training—including any expenditure that is legitimately part of the initiative—is charged against profit. EVA is then calculated as the Net Operating Profit After Tax (NOPAT) minus the Weighted Average Cost of Capital (C) as adjusted by a range of proprietary adjustments (K) that are provided as a service by Stern & Stewart [McClure 2003].

Those adjustments include such things as the "amortization of goodwill or capitalization of brand advertising." The advantage of EVA is that it produces a single financial index that can be used to characterize a diverse set of potentially contradictory directions [McClure 2003, Pettit 2001]. Approached as a tradeoff between total investment cost and potential value, EVA is a good way to gauge the impact of any process such as assurance on overall profitability. Beyond the general cost/benefit view however, EVA is really only useful when it leads into the use of another more precise valuation methodology [Mayor 2002].

Economic Value Sourced (EVS) – Cawly & the Meta Group

EVS sets out to quantify the value gained for every dollar invested [Meta Group 2000]. The investment in software assurance is always speculative because the risk and reward structure is hard to quantify. For instance, how do you assign a quantitative value to the increased customer trust that a secure software assurance function provides [Meta Group 2000]? In response to questions like that, EVS extends the analysis beyond the EVA approach by factoring risk and time considerations into the equation [Mayor 2002].

EVS assumes that IT investment decisions can be valued based on three strategic factors: reduction of risk, increase in productivity, and decrease in cycle time [Meta Group 2000]. Traditional return on investment (ROI) measures such as risk reduction savings or marginal productivity increases are the typical basis for quantifying value.

In addition, EVS adds standard timing factors such as flexibility. For instance, EVS asks such questions as "If the investment represents continuing cost, how quickly can those costs be adjusted to decreases in profitability" [Meta Group 2000]? Finally, risk-based considerations, such as the overall impact of the proposed investment on performance, interoperability, resiliency, or security of the operation are also factored in [Meta Group 2000].

EVS is an attractive approach because it allows for considerations outside of the traditional economic rate of return—considerations through which many of the indirect, abstract, or qualitative economic benefits of investment in software assurance can be understood and justified.

Total Cost of Ownership (TCO) – Gartner

Total Cost of Ownership (TCO) is one of the older, and more traditional, cost-based valuation approaches. It assesses an investment based strictly on its total direct and indirect costs. TCO aligns those costs with ongoing business performance in order to evaluate total value but does not assess risk or provide a means to ensure alignment with business goals [Mayor 2002].

When incorporated with a classic financial analysis such as ROI, TCO can provide a true economic value for any given investment. TCO takes a holistic view of total organizational cost over time. Ideally, it will let the manager calculate a projected rate of return on any investment based on the initial capital outlay, as well as all the aspects of the continuing cost of operation and maintenance [West 2004]. That cost estimate typically includes such ancillary considerations as physical space, security and disaster preparedness, training, and ongoing support. That's why TCO is sometimes referred to as Total Cost of Operation [Bailey 2003].

Benefit is generally calculated using an estimate of the cost that would accrue if a function or service were absent. For instance, TCO asks what the cost to the organization would be if a system failed or experienced a security incident. It then treats that cost value as a risk avoidance benefit [West 2004]. By treating incident cost that way, TCO provides a good running benchmark of the financial value of an overall risk mitigation program for software assurance.

TCO can be used to monitor the overall effectiveness of any assurance program by comparing the running cost of maintaining a given level of security to existing financial data about the cost of the incidents the program is designed to prevent [Mayor 2002]. For instance, if a given level of assurance is established to prevent buffer-overflow attacks, the national average cost of those attacks can be used as an index of the benefit that would be gained by preventing them.

Because it is strictly cost centered, TCO is best used for cost rather than value estimation. However, TCO also works well in conjunction with methodologies such as the Balanced Scorecard to provide an easy to understand picture of the cost side of the proposition.

ENVIRONMENTAL/CONTEXTUAL MODELS

These methods, sometimes called heuristic models, add subjective and qualitative elements to the mix. Their aim is to assign a quantitative value to such intangible qualities as environmental or contextual influences, including factors

such as human relations considerations and the affects of other organizational processes.

Balanced Scorecard - Norton and Kaplan

The Balanced Scorecard, conceived by Robert Kaplan and David Norton [Kaplan 1993] is arguably one of the easiest and most popular valuation approaches. Kaplan and Norton wanted to integrate traditional financial indicators with operational metrics and then place the results within a broader framework that could account for intangibles like corporate innovation, employee satisfaction or the effectiveness of applications [Kaplan 1996].

At its core, the Scorecard seeks to establish a direct link between business strategy and overall business performance [Berkman 2002]. It does that by balancing the standard financial indicators against essential, but more fluid, qualitative indicators such as customer relationship, operational excellence, and the organization's ability to learn and improve [Berkman 2002]. Thus, the Balanced Scorecard allows for ongoing assessment of the value of intangibles [Berkman 2002]. Furthermore, by requiring that every operational step be traceable to a stated strategic goal, it facilitates decisions about changes to that resource as conditions change [Kaplan 1992].

In practice, the organization's "scorecard" is customized for each operation by means of a planning process whose mission is to develop measures that capture primarily nonfinancial perspectives. Since this customization depends on the situation, there is no fixed set of quantitative measures. However, in every case, there are three or four appropriate metrics for each of the four scorecard perspectives, which are (1) financial, (2) customer, (3) internal business process, and (4) learning and growth. These perspectives are described in more detail on the Management and Accounting Web site.

The important point about using the Balanced Scorecard is that its metrics do not come in a "one size fits all" form. Generally, they come in three types. The first type includes those used to describe internal technical functions. Such a description is needed to judge technical performance against strategic goals. Examples of this type of metric include highly focused items such as reliability, processing speed, and defect rate [Mayor 2002]. These measures are not particularly useful to nontechnical managers, but they are objective and easy to aggregate into information that can help technical managers assign value to the IT function [Berkman 2002].

The second type of metric comprises those that normally come in the form of comparisons or "report cards" and are intended for use by senior executives [Kaplan 1992]. For example, if software assurance is considered a cost center,

the goal is either to show how those costs have improved over time or to describe how they compare with similar costs in similar companies [Kaplan 1992]. Examples of concrete measures in this area include personnel or service costs broken out on a per-user or other kind of index basis [Berkman 2002].

The final type of metric includes those intended for use by the business side of the company [Berkman 2002]—things such as demand and use statistics, utilization analyses, and cost and budget projections. These measures almost invariably tend to be unique to each business unit [Kaplan 1992].

The important point, however, is that the Balanced Scorecard allows an organization to value all of its assets appropriately. This is essential if the organization wants to prioritize and assign security protection to the full range of those assets, not just the tangible ones. With that goal in mind, an organization can begin to collect data or analyze existing information formulated from discrete measures to support the relative valuation of its information assets.

Customer Index: Andersen Consulting

Andersen Consulting's Customer Index method is aimed at helping companies determine the true economic value of any particular investment by referencing it to the customer base. It does that by tracking revenue, cost, and profit on a per-customer basis. The Customer Index collects data about those items and actively associates that data with changes on a per-customer basis [Eisenberg 2003].

The organization can use this index to estimate how a prospective decision might influence the various elements of its customer base. That estimation helps the organization determine the overall value of any investment by indexing it to how it has affected, or will affect, its customer base [Eisenberg 2003]. That requires the company to calculate the current cost and profitability of all of its functions on a per-customer basis. The index allows the company to estimate what any prospective investment might do to those numbers [Eisenberg 2003].

This approach isn't typically relevant to companies with just a few customers, but it is appropriate for any company where customer satisfaction drives every aspect of the business. More importantly, it has the potential to rationalize software assurance in terms that are intuitively realistic to business executives, whose primary goal is to increase market share [Mayor 2002].

Thus, the ability to differentiate the value of a certain set of assurance practices for a given product in terms of the impact on the customer base is a very persuasive argument for any business case. Nevertheless, the additional cost of maintaining a continuous and accurate accounting of revenue and expense on a per-customer basis is a serious consideration in adopting this approach.

Information Economics (IE) - The Beta Group

IE has a strategic focus. Its goal is to force managers to agree on and rank their spending priorities at the corporate level. IE does that by forcing managers to draw specific conclusions about the strategic business value of individual initiatives [Benson 1992].

IE requires a discrete value estimate for every project [Parker 1989]. That estimate is then compared across several projects based on standard economic descriptions like Net Present Value. The benefit of IE is that it provides a total relative value for each project in the portfolio. It helps decision makers to objectively assess the value of their profile of systems side by side, which should then let them allocate resources where they can do the most good [Benson 1992, Parker 1989].

IE is based around the characterization of a hierarchy of places where benefit can be derived [Benson 1992]. At the highest level, there are intangible things such as risk reduction and enhanced ROI. Further down the hierarchy, there are also hard measures such as cost and revenue. Managers prepare a list of decision factors [Parker 1989] that clearly express the benefit as a value; for example, "reduces cycle time by 'X' percent [Benson 1992]. Vague statements such as "will save time" are not allowed.

These decision factors, which are often scenario driven, are evaluated individually based on their relative value or risk to the business. Intangibles such as competitive responsiveness or the value of management information are assessed against a range of contingencies [Benson 1992]. Risk is typically expressed by means of a likelihood versus/impact analysis. In effect, strategic decisions can then be referenced to that quantitative ranking [Parker 1989].

IT Scorecard – Bitterman, IT Performance Management Group

This is a performance measurement system similar to the Balanced Scorecard. Its aim is to let the organization track the IT operation's financial contribution and alignment with corporate strategies. Its overall goal is to understand the IT function's organizational strengths and weaknesses [Leahy 2002].

This approach is different from the Balanced Scorecard in that it focuses strictly on IT. Its aim is to provide a strategic basis for evaluating the IT function that is independent of all other business, or organizational considerations [Leahy 2002]. The approach is therefore bottom up from the internal IT view. The organization must clearly demonstrate how much value each IT function or process contributes to the overall business value. But, as we have seen, effective IT financial metrics are hard to find, since IT involves so many abstract and dynamic elements. That lack of measurement is one of the main reasons why IT has tradi-

tionally been viewed as a cost rather than as a resource [Leahy 2002]. Thus, the IT Scorecard focuses its measurement activity on metrics that characterize what IT brings to the business.

The intent of this approach is to communicate the value of IT rather than its cost [Bitterman 2006]. The measures used concentrate on capturing all the leading indicators of value that support the achievement of the company's strategies; for example, how fast a help desk responds to a problem and how often that problem is fixed [Bitterman 2006].

Like the Balanced Scorecard, the IT Scorecard also introduces the concept of external comparative measures and benchmarks in order to create meaningful IT performance metrics [Bitterman 2006]. The aim of the IT Scorecard is to determine how effectively current IT resources are supporting the organization and, at the same time, to assess ways that IT can better respond to future needs.

The IT Scorecard revolves around five perspectives: mission, customers, internal processes, technology, and people/organization [Bitterman 2006]. The first step in the value assignment process is to precisely characterize what the business wants out of the IT function as well as what IT can feasibly bring to the business. That description is used to establish organization-wide consensus on the metrics that will be required to capture that value.

The metrics themselves must accommodate the fact that a change in one area can have an effect on the value of another area. Thus, most successful scorecards developed through this approach are the result of numerous iterations that work toward getting this tradeoff right [Leahy 2002]. An initial set of metrics can be evolved out of this process into a group of more sophisticated measures that give greater insight into business value. However, effective measurement programs can only be customized to the strategies they support. That is the one serious weakness in this approach. The IT Scorecard can never be used right out of the box, since it requires an organization to develop and then maintain a custom set of metrics [Mayor 2002].

QUANTITATIVE ESTIMATION MODELS

Real Options Valuation (ROV)

Real Options Valuation (ROV) aims to put a quantitative value on operational flexibility. It allows an organization to value any investment that will underwrite or create a more relevant and responsive operation [Luehrman 1998a]. Thus, ROV can be used to value technological investment.

ROV centers on ensuring maximum flexibility in the deployment of technological assets. Using this approach, an organization can determine the value of an investment by focusing on the likely consequences of a particular action over time (assuming that these consequences can be described in probabilistic terms) [Luehrman 1998a].

In most instances, those outcomes are characterized by assumptions about future performance. However, no set of assumptions is going to provide a perfect forecast. The best approach to the ROV process is to derive a value for every feasible option [Luehrman 1998a].

As a consequence, much of ROV involves identifying every factor that might be involved in or impacted by a given decision and then estimating the likelihood of occurrence. Thus, ROV is based on

- decision variables - assumptions that are under the specific control of the decision makers and can be adjusted to increase project value as required
- stochastic assumptions - assumptions that are random variables with known or estimated probability distributions
- deterministic assumptions - assumptions that are based on established benchmarks [Luehrman 1998b]

Real options have concrete outcomes. Thus the decision rules for a exercising a real option must be referenced to observable behaviors that can be used to assess the performance of every variable associated with it. These behaviors must be observable and documented for a given period prior to the point where the decision is made [Luehrman 1998a]. For example, a decision to add an assurance practice might be based on the known occurrences and costs of the threats that practice was meant to address over the past year of operation [Neely 2001].

The problem with ROV is that it is, by necessity, complex, so it works best in situations that are well defined or where experience exists. Thus, ROV models are effective in estimating the likelihood of stock options or pork bellies [Luehrman 1998b]. However, since the process of assurance is not yet well understood, the construction of the finite model for it is, at best, an exploratory effort [Neely 2001].

Applied Information Economics (AIE) – Hubbard

AIE is perhaps the most rigorously quantitative methodology in this set [Kwon 2001]. It centers on the use of probabilistic models to reduce uncertainty [Hubbard 1997]. It is assumed that if the appropriate amount of data can be collected (or estimated), it is possible to calculate the fiscal value of any option [Hubbard 1997].

Since all decisions involving deployment of the software assurance function involve the estimation of probabilities of both benefit and failure, it is hypothetically possible to build a sufficiently accurate picture of the financial risks and returns of any given decision option, or a related set of options, using AIE. This will allow the decision maker to understand the exact probabilities of success. This knowledge can then theoretically allow decision makers to balance their assets and activities in such a way that they will exhibit the best risk-reward characteristics [Hubbard 1997].

The analysis process itself involves classic actuarial estimation. Actuarial statistics are used in order to quantify the consequences of a given decision, which provides a proper understanding of risk and return.

Applied Information Economics computes the value of additional information. The aim is to model uncertainty quantitatively and then compute the value of marginal uncertainty reductions [Hubbard 1999]. The AIE process is based on Hubbard's Clarify, Measure, Optimize approach [Hubbard 1997], which aims to isolate and clarify the precise set of variables that are involved in and affect the decision. Such isolation and clarification allows AIE to provide specific information for decision makers.

For example, most decisions about software assurance are made based on the probability of harm. Thus, a manager might estimate that a given program would have a likelihood of 20% of failing or being exploited. AIE would restate that estimate in terms of the probabilities that a certain type of virus would be able to exploit that code, versus the likelihood that it could be compromised by a range of other attack types [Hubbard 1997]. This sort of detail makes it easier to estimate the long-term value of the decision to increase or decrease the assurance activity.

AIE analysis is considered by its proponents to be the only truly scientific and theoretically based methodology available. Its ideal outcome is an actuarial risk-versus-return statement about the probabilities of the success of a given decision [Mayor 2002]. In order to do that, AIE integrates classic principles of economics, actuarial science, and decision theory into a single approach that theoretically supports proper decision making about how to conduct business operations.

CoCoMo II and Security Extensions – Center for Software Engineering

CoCoMo II, a cost estimation technique that dates back to 1991, is the flagship for software engineering economics. It consists of a hierarchy of three increasingly detailed and accurate forms. It was designed by Barry Boehm to give an estimate of the number of programmer-months it would take to develop a software product.

CoCoMo has been revised extensively over the past 25 years. There was an effort to incorporate security extensions, but this additional development work has been terminated without completion or validation. We include it here because it is a good approach technically. Completion of this approach or development of a similar approach, along with validation and tool support, could be very useful.

The changes and extensions, which are risk-characterizing factors, are plugged into the model to obtain the estimates. The security components are delimited by the 13 security functions defined in ISO 15408, which is generally called the Common Criteria [Colbert 2002]. These security functions produce a standard Evaluated Assurance Level (EAL) that can be compared across products. Nevertheless, the intent of the security extensions was to simply use those criteria categories as the basis for defining the expected functionality, rather than produce an EAL [Colbert 2002].

The estimation itself is driven by a set of stock adjustment factors in the same fashion as the classic CoCoMo process. Essentially, software size and security size are factored into an estimate of the total amount of LOC programmer hours (or cost) required to produce it. As with traditional CoCoMo, a properly calibrated process would provide an explicit estimate of the cost that will be required to add a given amount of software functionality to the project [Madachy 2002].

There are several problems with the general CoCoMo approach. First, it has little recognition outside of the software engineering community, so it has to be "popularized" with traditional managers. Second, because the multiplier factors should be calibrated to the environment, CoCoMo does not work in unstructured operations. Thus, it is essential that the operations they are applied to execute in a systematic and reliable way. Since the term "chaos" seems to best fit the situation in most commercial software operations, the second problem is a showstopper.

Finally and most importantly, CoCoMo is too explicit to be useful as a general process cost estimate. As it is now constituted, CoCoMo provides an estimate of the effort cost of adding additional security functionality to a piece of software. It does not embody variables that factor in the additional cost of the software assurance process per se. If those costs were to be added, they would obviously be part of the multiplier factors themselves. There is some indication that the risk factors themselves are useful in identifying areas of potential exploitation [Madachy 2002]. However, the ability to actually valuate those factors is not yet advanced enough to be reliable.

FINAL OBSERVATIONS: SOME COMMON FEATURES

Although these models represent a range of approaches, they share some common elements that should be noted for the purpose of value estimation.

General Factors

Holistic representation - First and perhaps most important, almost all of these models incorporate qualitative, business-oriented considerations along with quantitative factors such as cost. These considerations and factors are expressed primarily as risk versus return, but the consideration of non-tangible items, such as business priorities, is also built into the process.

Quantitative risk assessment - Risk assessment in a probabilistic sense seems to be a critical driver for almost all of these models. In that respect, the value of the investment is expressed in terms of the degree of risk avoidance that a software assurance activity can demonstrate.

Continuous execution - Valuation and risk assessment is a continuous process in every one of these models. That is because the threat environment is constantly changing, and thus, the assurance requirement is dynamic. The risk assessment is meant to support the efficient deployment of resources to mitigate priority threats to any asset of value. It should therefore be systematic and rigorous and must be an institutional process within the organization's business model.

Standard metrics - the importance of a standard set of metrics, mutually agreed on and commonly understood, is a common thread in all of these models. Therefore, any valuation process has to begin with the development of a standard set of measures that are consistently applied across time in the practical valuation process. These measures must be maintained appropriately over time and updated immediately as conditions change.

Common Factors Across Models

Flexibility - Any process that enhances an organization's ability to recognize and respond appropriately to events as they arise appears to be valuable. This flexibility is characterized by the detailed understanding of all relevant decision options and the existence of enough information about each one to support making the right choice.

Likelihood - The ability to accurately estimate the likelihood of occurrence is essential. That implies the need for enough focused baseline operating data to support stochastic estimates. It also implies the requirement to develop commonly agreed on metrics prior to the actual statistical forecasting process and to collect sufficient standard data to support estimates of probability for any valuation activity.

Granularity - When it comes to the level of focus, there are two opposing trends in these models. First, there is a trend toward value estimation based on high-level alignment with business goals and prioritization of requirements. Second, there is a trend toward decomposition of the decision process into its constituent variables at the lowest practical level of understanding. The first trend supports quicker understanding but lacks precise valuation. The second trend supports more accurate valuation but requires intensive data collection.

Decision Criteria - All decision rules must be stated explicitly. Since valuation primarily involves subjective assessment, the role of the decision criteria is to provide a common basis for understanding the implications of any given proposition. Criteria are soft in the sense that they have to be developed, so it is essential that all criteria are documented prior to any operational valuation activity.

Business Value - Intangible value has to be quantified. This can be done through a number of subjective methods including Delphi, business owner benchmarking, or anecdotal observation with averaging. Regardless of the approach used, the subjective value estimate has to be systematically executed and rigorously controlled. However, the principle benefit of software assurance is expected to be increased business value, which must be measured in some objective sense.

LIMITATIONS

Note that many of these models assume that we can accurately predict the probability of an event. As we all know, predicting the probability of a Cyber attack can be difficult. Oftentimes, the best we can do is to produce rough estimates on the basis of previous data. Since attackers do not want to be detected, previous data on attacks is often incomplete, and hence the associated predictions can be based on flawed data.

Calculating risk is not as straightforward as some of the models suggest. To do it, you must have an understanding of the actual threats, vulnerabilities, and probability of exposure. Such data is not easy to come by. Moreover, the nature of the risks will change as we shift from individual hackers trying to get attention to criminals motivated by financial gain or terrorists with other motivations. The Architectural Risk Analysis and System Strategies content areas of BSI discuss risk assessment and may provide assistance in this area.

Bruce Schneier believes that it is not feasible to accurately calculate the benefit that is derived from improved security. He points out that there is very little actual data on the cost of a break-in and that predicting the cost of a rare but damaging event is fraught with peril. In this article he summarizes his position on

calculating security ROI as follows: “It's a good idea in theory, but it's mostly bunk in practice.”

CONCLUSIONS AND FUTURE PLANS

We are not in a position to recommend a specific model. We have presented a survey of available models for BSI readers to consider. The “ideal” model for calculating the cost and value of software assurance may be one of these, or it may be a new model that builds on the common features that we have discussed. In 2008 we conducted a workshop on Business Case, and all indications are that there is no single common model that is widely accepted. Microsoft is using the level of vulnerabilities and patches needed as a measure of improved cost/benefit [Microsoft 2008]. Data presented by Fortify indicates that the cost of correction of security flaws at the requirements level is up to 100 times less than the cost of correction of security flaws in fielded software.

Subsequent to the workshop, we developed a guide for Making the Business Case for Software Assurance. We encourage BSI readers to use this report in their efforts.

BIBLIOGRAPHY

[Anderson 2001]

Anderson, Ross. *Why Information Security Is Hard–An Economic Perspective*. Computer Laboratory, University of Cambridge, 2001.

[Apfel 2003]

Apfel, Audrey. “The Total Value of Opportunity Approach.” *CIO*, January 15, 2003.

[Bailey 2003]

Bailey, John & Heidt, Stephen R. “Why Is Total Cost of Ownership (TCO) Important?” *CSO*, November 2003.

[Benson 1992]

Benson, Robert J. *Information Economics and the Business Value of Computers* (POSPP Report P-34-1). Dallas, TX: Chantico Publishing, January 1992.

[Berkman 2002]

Berkman, Eric. “How to Use the Balanced Scorecard.” *CIO*, May 15, 2002.

[Bitterman 2006]

Bitterman, Michael. *How IT Benefits From Adopting Measurement-Management Techniques*. ITPMG, 2006.

[Brynjolfsson 2003]

Brynjolfsson, Erik & Hitt, Lorin M. *Computing Productivity: Firm-Level Evidence* (Working Paper No 4210-01). Cambridge, MA: MIT Sloan School of Management, June 2003.

[Cavusoglu 2006]

Cavusoglu, Huseyin; Cavusoglu, Hasan; & Zhang, Jun. "Economics of Security Patch Management." Workshop on Economics of Information Security (WEIS). Cambridge, England: Robinson College, University of Cambridge, June 2006.

[Colbert 2002]

Colbert, Ed; Reifer, Don; & Gangadharan, Murali. "COCOMO II Security Extensions." 17th International Forum on COCOMO and Software Cost Modeling. Los Angeles, CA, October 2002.

[CNSS 2006]

Committee on National Security Systems (CNSS). "National Information Assurance (IA) Glossary." Instruction No. 4009, 2006.

[CSTB 2000]

Computer Science and Telecommunications Board (CSTB). *The Digital Dilemma: Intellectual Property in the Information Age*. Washington, DC: National Academies Press, 2000.

[Cummings 2002]

Cummings, Joanne. "IT Portfolio Management." *Network World Fusion,* April 2002.

[Curtis 1995]

Curtis, W. "Building a Cost-Benefit Case for SPI Revised." *Proceedings of the 7th SEPG Conference*. Boston, MA, May 1995.

[Datz 2003]

Datz, Todd. "Portfolio Management, How to Do It Right." *CIO,* May 2003.

[DiDio 2005a]

DiDio, Laura. "Enterprises Reap Value from Software Assurance Services, Training and Flexible Payments." Yankee Group, January 2005.

[DiDio 2005b]

DiDio, Laura. “Mirosoft Software Assurance Upgrade Program Gains Traction and User Acceptance.” Yankee Group, January 2005.

[Dynes 2006]

Dynes, Scott; Andrijcic, Eva; & Johnson, M. Eric. “Cost to the U.S. Economy for Information Infrastructure Failures.” Workshop on Economics of Information Security (WEIS). Cambridge, England: Robinson College, University of Cambridge, June 2006.

[Eisenberg 2003]

Eisenberg, Bryan. “How Are You Measuring Customers?” *ROI Marketing*, February 2003.

[Feather 2001]

Feather, M. S.; Sigal, B.; Cornford, S. L.; & Hutchinson, P. "Incorporating Cost-Benefit Analyses into Software Assurance Planning," 62-68. *Proceedings of the 26th Annual NASA Goddard Software Engineering Workshop*, IEEE Computer Society, 2001.

[Gibbons 2004]

Gibbons-Paul, Laura. “How to Make Your Best Case.” *CIO*, February 2004.

[Giera 2004]

Giera, Julie. “Microsoft Licensing: More for the Money.” Giga Research, February 2004.

[Giga 2006a]

Giga Research. “Total Economic Impact of Microsoft’s Software Assurance.” Cambridge, MA: Forrester Research, Inc. (July 2006).

[Giga 2006b]

Giga Research. “Forrester Software Assurance ROI Tool, User's Guide, and Report: Calculating the Value of Software Assurance.” Cambridge, MA: Forrester Research, Inc., July 2006.

[Hubbard 1997]

Hubbard, Douglas. “Everything is Measurable.” *CIO Enterprise Magazine*, November 1997.

[Hubbard 1999]

Hubbard, Douglas. "Checks and Balances: Measuring the Value of Technology Investment." *CIO,* April 15, 1999.

[Kaplan 1992]

Kaplan, Robert & Norton David. "The Balanced Scorecard: Measures that Drive Performance." *Harvard Business Review 70,* 1 (1992).

[Kaplan 1996]

Kaplan, Robert & Norton, David. "Using the Balanced Scorecard as a Strategic Management System." *Harvard Business Review* (Jan-Feb 1996): 75-85.

[Kaplan 1993]

Kaplan, Robert & Norton, David. "Putting the Balanced Scorecard to Work" *Harvard Business Review,* September-October 1993: 134-147.

[Kitchenham 1996]

Kitchenham, Barbara & Pfleeger, Shari Lawrence. "Software Quality, the Elusive Target", *Software 13,* 1 (January 1996): 12-21.

[Konary 2005]

Konary, Amy. "Atos Origin: A Microsoft Software Assurance Case Study." Framingham: MA: International Data Group (IDG), August 2005.

[Kwon 2001]

Kwon, Regina. "The Probability Problem." *Baseline Magazine,* December 2001.

[Leahy 2002]

Leahy, Tad. "IT Measures Evolve." *Business Finance,* March 2002.

[Luehrman 1998a]

Luehrman, Timothy A. "Investment Opportunities as Real Options: Getting Started on the Numbers." *Harvard Business Review,* July-August 1998.

[Luehrman 1998b]

Luehrman, Timothy A., "Strategy as a Portfolio of Real Options." *Harvard Business Review,* September-October 1998.

[Madachy 2002]

Madachy, Ray and Stutzke, Dick. "Use of Cost Models in Risk Management." 17th International Forum on COCOMO and Software Cost Modeling. Los Angeles, CA, Oct. 2002.

[Mahmood 2004]

Mahmood, Mo Adam; Kohli, Rajiv; & Devaraj, Sarv. "Measuring Business Value of Information Technology in E-Business Environments." *Journal of Management Information Systems 21*, 1 (Summer 2004): 11-16.

[Mayor 2002]

Mayor, Tracy. "A Buyer's Guide to IT Value Methodologies." *CIO Magazine*, July 2002.

[McClure 2003]

McClure, Ben. "All About EVA." Investopedia.com, March 2003.

[McGibbon 1999]

McGibbon, Thomas. "A Business Case for Software Process Improvement Revised." Rome, NY: DoD Data Analysis Center for Software (DACS), September 1999.

[Meta Group 2000]

Meta Group. "Leadership beyond the Project." Stamford, CT: Meta Group, Gartner, 2000.

[Microsoft 2005]

Microsoft. "Build an Airtight Business Case for New IT Investments." Redmond, WA: Microsoft, December 2005.

[Microsoft 2008]

MSDN. The Microsoft Security Development Lifecycle (SDL): Measurable Improvements for Flagship Microsoft Products, 2008.

[Neely 2001]

Neely, James. "Hybrid Real Options Valuation of Risky Product Development Projects." Cleveland, OH: Booz-Allen & Hamilton, 2001.

[Ozment 2006]

Ozment, Andy & Schechter, Stuart E. "Economic Barriers to Adopting New Security Protocols." Workshop on Economics of Information Security (WEIS), Cambridge, England: Robinson College, University of Cambridge, June 2006.

[Park 2006]

Park, Alvin R. "Determining the Value of Microsoft Software Assurance." Gartner, April 2006.

[Parker 1989]

Parker, Marilyn M & Benson, Robert J. “Enterprisewide Information Economics.” *Journal of Information Systems Management 6*, 4 (Fall 1989): 7-13.

[Pettit 2001]

Pettit, Justin; Dower, John; Pichler, Karl; & Perez, Jorge. “EVA and Corporate Portfolio Strategy.” *EVAluation 3*, 9 (December 2001).

[PITAC 1999]

President's Information Technology Advisory Committee (PITAC). "Information Technology Research: Investing in Our Future.” Arlington, VA: President's Information Technology
Advisory Committee, February 1999.

[Schwartz 2000]

Schwartz, Eduardo S. & Zozaya-Gorostiza, Carlos. “Valuation of Information Technology Investments as Real Options.” *Finance*, November 2000.

[Wang 2006]

Wang, R. & Erickson, J. “The Financial Impact of Packaged Applications, a Tool for Comparing the ROI of Enterprise Applications.” Cambridge, MA: Forrester Research, Inc, July 2006.

[West 2004]

West, Richard & Daigle, Stephen L. “Total Cost of Ownership: A Strategic Tool for ERP Planning and Implementation.” Philadelphia, PA: Center for Applied Research (CFAR), January 2004.

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM-0001120