Total Cost of Security – A Method for Managing Risks and Incentives Across the Extended Enterprise

Russell Cameron Thomas
Principal, Meritology
1534 Plaza Lane, Suite 306
Burlingame, CA, 94010
1-650-692-2731
russell.thomas@meritology.com

ABSTRACT
This is an extended abstract of the presentation of the same title for the Cyber Security and Information Intelligence Research Workshop, 2009.

Categories and Subject Descriptors

General Terms

Keywords
Information Risk Management, Cyber Security, Total Cost of Security, Loss Distribution Approach

1. INTRODUCTION
One of the main challenges facing information technology (IT) managers and business executives is how to map security metrics and performance to business metrics and performance. This is necessary to align business goals and investments with security requirements, and to balance risks against costs and rewards. Lack of such metrics has resulted in a persistent disconnection between business decision-makers and security specialists regarding value and risk of information security [1].

Because the benefits of security are the avoidance of uncertain losses, applying traditional cash flow return on investment (ROI) techniques would be inappropriate, confusing, or misleading. Even variations tailored for security (e.g. Return on Security Investment, ROSI [3], have fundamental problems.) Furthermore, the domain is rife with unruly uncertainty (i.e. ambiguity, incomplete information, contradictory information, intractability, unknown-unknowns, etc.) which makes it difficult or impossible to reliably estimate annualized loss expectation (ALE) or other probabilistic estimates of expected losses.

As a solution, I propose a managerial accounting framework called “Total Cost of Security”. (The name alludes to the Total Quality Management and the concept of “Total Cost of Quality”.)

The proposed method has the following advantages over previous methods:

- It is compatible with both Generally Accepted Accounting Practices (GAAP) and modern ERP packages.
- It is compatible with enterprise risk management (ERM) frameworks.
- It is compatible with economic theories of the firm and rational decision-making with uncertain and incomplete information.
- It provides a general framework for integrating a variety of “ground truth” security metrics into an economically meaningful composite measure.
- It significantly reduces the data collection burden compared to other approaches (e.g. ALE).
- It makes the most of available information and avoids many of the problems of unruly uncertainty.
- It is robust to changing threat, vulnerability, asset, and organization environments.
- It supports a variety of incentive instruments for stakeholders to both manage risks better, minimize externalities, and to disclose relevant information.
- It is composable, which allows modular analysis of complex organizations and networks both at a component level and at various levels of aggregation.
- It can be extended to include related risks such as privacy, intellectual property protection, and digital rights.
- It is applicable to a wide variety of organizations, including for-profit, not-for-profit, government, and military. It scales well across organization size and structures, including networks of organizations.
2. PREVIOUS METHODS
There have been previous attempts to quantify the risks associated with information security including Return on Investment (ROI), Discounted Cash Flow (DCF), Return on Security Investment (ROSI), and Annualized Loss Expectancy (ALE) and variants. Each of these has severe or fatal limitations when applied to information security risk. Only the ALE method is consistent from an economic perspective. However, it is not widely implemented because of the difficulty of getting enough historical data to estimate probabilities of loss for each incident or loss type. There are other severe problems with the ALE method, including the lack of any way to account for the dependence structure between incident types. This leads to significant underestimation of “tail risk”.

Given the difficulty of quantifying information security risk, many organizations and analysts rely on qualitative risk assessment methods, including the “Frequency vs. Severity” 3X3 Qualitative Matrix (with “High-Medium-Low” values for each dimension). These are easier to produce and are useful for informing some decisions, but they lack the power of quantitative risk measures. In particular, it’s not easy to use them as a basis for incentive instruments and they don’t compose easily.

3. REQUIREMENTS
The requirements for a risk management framework were listed in Section 1, phrased in the form of “advantages”. More technically, it needs to be based on coherent risk measures, with the properties of translation invariance, subadditivity, positive homogeneity, and monotonicity [4].

In addition, there is the requirement to harmonize two perspectives of economic risk. The first perspective is that of the rational investor who is focused on short-term returns, and volatility of returns. Performance is defined as return on investment, and it is determined by the “fat of the curve” characterized by the mean and variance of return distributions.

The second perspective is the insurance actuary who is focused on long-term funding of a pool of risks. Performance is defined as avoiding “ruin” (i.e. paying out more in claims than you take in as premiums), and is determined by the “tail of the curve” characterized by parameters that quantify the thickness of the probability distribution at extreme values.

Unlike previous methods, the Total Cost of Security framework harmonizes these two perspectives on economic risk to support rational decision-making and incentive instruments.

4. TOTAL COST OF SECURITY FRAMEWORK
This framework is based on the Loss Distribution Approach (LDA) that has become common in Enterprise Risk Management (ERM), pioneered in the financial services industry. The curve in Figure 1 is a forward-looking probability density function for total cost of security for a given period.

![Figure 1. Idealized Total Cost of Security Probability Distribution](image)

It’s a matter of policy what costs to include or exclude in Total Costs of Security. The framework is intended to be broad and inclusive, and it can include:

- Direct costs of information security (personnel, security-specific operating and capital expenses, professional services, security training and awareness programs, security measurement and management costs, etc.)
- Indirect costs of information security, allocated proportionately (IT help desk, configuration management, patch management, etc.)
- Direct costs of security breaches, intrusions, losses, and recovery (discovery, damage control, emergency response, system restoration, penalties and/or fines, etc.)
- Indirect costs of security breaches, intrusions, losses, and recovery, including revenue impact, reputation damage, etc.)

Our first innovation is to divide security-related or cyber trust costs into three categories: “Budgeted”, “Self-insured”, and “Catastrophic” (Figure 1). Basically, this approach divides the aggregate cost probability distribution into three sections. The fat part of the curve near the mean is "budgeted". The tail section up to some threshold (95% or 99%) is "self-insured". The very far end of the tail is "catastrophic". Therefore, any given incident type, vulnerability, or threat could contribute costs into any or all of these categories.

- "Budgeted" region is the “fat” part of the curve that includes costs that are predictable and likely within the budget year. This includes all direct spending on security, plus indirect costs, plus the expected value of all high frequency losses and some small mix of lower frequency losses. It also includes the opportunity costs – business activities that are prevented or inhibited by security.

- "Self-insured" region covers loss magnitudes are potentially big enough to bust the budget (i.e. material to quarterly earnings statements), or could get the firm on the front page of a national newspaper, or could even threaten the firm’s credit rating, but not necessarily
threaten firm survival. These losses are low probability, but not close to zero.

- "Catastrophic" region covers the most extreme loss values that are very unlikely and/or very unpredictable, but could threaten firm survival or even more widespread systemic losses. This includes most or all “doomsday” scenarios.

The second innovation is the treatment of indirect costs, especially indirect costs of security incidents. We advocate a general method of valuation called “Expected Cost of Recovery” – the anticipated cost of restoring the information systems, data, business processes, and business relationships to their previous level of capability and performance. This is more conservative and reliable than other measures which try to estimate the lost business value due to the security incidents, including decline in stock prices and other stakeholder value metrics.

5. TCoS Risk Measure

The general formula for TCoS (short for Total Cost of Security, pronounced “TEE-koss”) is summarized by the following equation:

\[ \text{TCoS} = B + SI + C \]

where

- \( TCoS \) is the Total Cost of Security risk measure
- \( B \) is the budgeted security costs and losses for the period (i.e. median costs, or within a margin of the median),
- \( SI \) is the self-insurance premiums to cover low probability-high impact losses, and
- \( C \) is the costs of business continuity to cover deal with catastrophic scenarios, allocated according to information security causes and effects.

In plain language, TCoS starts with expected spending on security and security-related costs (losses, etc.) that are reflected in an organization’s budget. Then add the cost of insurance premiums to cover losses low probability-high impact losses, but below the level of catastrophe. (Nearly all organizations will carry this risk rather than transfer it, so I call it “self-insurance”.) Finally, the cost of business continuity allocated to information security is added. Once these three components are added, the result is a TCoS in current dollars for the next time period. A stream of TCoS values over multiple periods can be treated like ordinary cash flows in the standard Discounted Cash Flow (DCF) method. The discount rate, a critical parameter, is very easy to specify – it’s the firms weighted-average cost of capital, or in other contexts, the risk-free rate. (In ordinary capital budgeting analysis, the discount rate in DCF is adjusted to match the riskiness of the project. “Riskiness of the project” is a tortured concept in the information security context.)

5.1 Decision Criteria

The most general decision criterion can be simply stated:

- “Minimize TCoS while meeting other business objectives”

It’s also possible to integrate TCoS into ordinary return on investment calculations to get a risk-adjusted return for various business opportunities or investments (e.g. outsourcing a business function, implementing a new intellectual property licensing revenue model for on-line media, etc.) that have significant information security implications.

In addition to this general decision criterion, TCoS can inform more complicated decisions and has well-defined methods of composition (i.e. combining TCoS measures from different organization units into a composite measure for the entire organization) using portfolio theory, and also risk budgeting (allocation and prioritization incentives and constraints to guide business unit managers). Details are outside the scope of this presentation.

5.2 Estimation Methods

Of course, the success of this or any other risk measurement method depends on our ability to estimate the relevant probability distribution curves. If no such method is feasible, either in theory or in practice, then the method should be rejected. In the proposed Total Cost of Security framework, these are still open research questions. In this presentation I propose a set of methods that seem feasible, or at least promising.

(It’s important to note that the Total Cost of Security framework does not depend on any particular estimation or modeling method.)

Rather than use a single estimation method for the whole curve (as in the DCF and ALE methods), I propose piece-wise approach. The probability distribution is then assembled from the pieces. Though each set of methods is different, they can draw from similar data: operational security metrics (a.k.a. “ground truth”), business process metrics, expert opinion, historical data of incidents and losses, estimates of asset value and other values at risk.

- The “Budgeted” region would be estimated using fairly conventional cost-driver models (i.e. linear relationships between operational metrics and indirect or overhead costs, etc.) and data drawn from accounting information systems.
- The “Self-insured” region would be modeled using rank order or order-of-magnitude approaches, possibly combining stochastic methods with inferential reasoning.
- The “Catastrophic” region would be modeled using scenario analysis and ordinal or nominal scales. Here, the precision of cost estimate is much less important than it’s the qualitative value to guide strategy and business continuity planning, for example.

An illustrative example is given for estimating self-insurance costs of data breaches for a mid-sized retailer (13 million credit card records). Source data could include statistics about the IT architecture and operations, security metrics, the company’s breach history, industry surveys and data breach databases, threat models, and business process models. Using methods such as Bayesian Networks, Delphi Method, Predictive Modeling, and Monte Carlo Simulation, it is possible to estimate the self-insurance quantile, including second order probabilities.  

Another illustrative example is given for how TCoS could be used to define incentive instruments in the extended enterprise for the same retailer, focusing on card payment processing.
The incentive instruments do not need to be linked to the complete TCoS metric for each party. Instead, contingent payments, pooling, and other incentives can be tied to thresholds and limits for TCoS or its components. There will be opportunities for third parties to support incentive instruments, including risk rating agencies and insurance companies, using facilities such as parametric (indexed) insurance [5] and finite risk insurance.

6. RESEARCH RESULTS
Theoretical research on the Total Cost of Security framework and TCoS risk measure is in the very early stages. We have a few promising research results based on computational simulation of hypothetical cases. Specifically, we can demonstrate the following theoretical results:

1. Demonstrated that TCoS is a coherent risk measure
2. Demonstrated that it is feasible to derive a stable, acceptable estimate of the “Budgeted” region of the Total Cost of Security distribution curve using cost driver methods from Activity-Based Costing, plus a formal bargaining game for cost sharing among (competing) stakeholders.
3. Proposed an approach to estimating of the “Self-insured” region of the Total Cost of Security distribution curve using a pluralistic, competition between diverse models. This method remains to be tested and validated.
4. Using similar methods as #2, demonstrated a method to segment TCoS and it’s components into three subcomponents: “internally-driven”, “partner-driven”, and “externally-driven”. These sub-components can serve as the basis for risk pooling, insurance, cap-and-trade, or other incentive-based mechanisms.

7. DISCUSSION
Of course, confidence in this whole proposal depends on empirical research and on whether available data sets can be used usefully to estimate TCoS. Our claim at this stage of research is that the framework is promising and seems to be viable from a theoretical perspective.

One of the advantages of the proposed Total Cost of Security framework is that it can incorporate any type of information security risk or, more broadly, cyber trust which includes privacy, intellectual property protection, and digital rights management.

It is also flexible enough to handle a wide range of risk profiles. In cases where the Total Cost of Security distribution curve happens to be normal distribution with relatively modest variance, then it would all fall into the “budgeted” category, and thus could be managed using traditional budget and cash flow methods. On the other hand, if the loss distribution has a “fat tail”, then the three-part approach becomes very useful to distinguish between what we know with confidence and what we know with less confidence or don’t know at all.

The framework makes the most of existing information, aligns with decision-making processes, and avoids the problem of conflating reliable and unreliable estimates. It requires innovations from Enterprise Risk Management, Activity-based Costing, and qualitative reasoning. The approach is roughly analogous to the Total Cost of Quality concept that helped motivate the Total Quality Management movement. In addition to helping with security cost and performance management, this approach highlights the importance of organization learning and discovery.

Another advantage is that it is compatible with existing methods for enterprise investment and performance management, including “Risk-adjusted Return on Capital” (RAROC) in financial services and “Economic Value-added” (EVA) across various industries. In essence, “self-insurance” adds to the capital required by a project or business unit. Higher levels of information risk mean a larger “self-insurance” pool is required, which lowers return on capital, and vice versa.

It may be possible to standardize these methods with industries and organization types to allow, for the first time, meaningful aggregation of cyber trust cost information to guide government policy and vendor product development decisions. It would also allow meaningful public disclosure of cyber trust risks and risk tolerance in stakeholder reports and regulatory filings.

8. ACKNOWLEDGMENTS
My thanks to Patrick Amon, Bob Austin, Sean Barnum, Jean Camp, Fred Cohen, Eric Dalci, John Delaney, Naomi Fine, Dan Geer, Alex Hutton, Jack Jones, Georgiy Bobashev, Ray Kaplan, John Nye, Elizabeth Nichols, Brent Rowe, and Digilio Simoni for their ideas, support, feedback, and suggestions. Additional thanks goes to the members of Securitymetrics.org for their comments, suggestions, and feedback.

9. REFERENCES