Applying ROI Analysis To Support SOA Information Security Investment Decisions

Kevin Buck
Diane Hanf
Prasant Das

2008 IEEE International Conference on Technologies for Homeland Security
Agenda

- Introduction
- SOA Information Security Challenges
- Addressing SOA Security Challenges
- Different Investment Decision-Making Approaches Yield Different Results
- Government Information Security Investment Decision-Making Challenges
- Government Application of ROI Principles
- SOA Information Security ROI Analyses
- Trust Domain Example
- Conclusions
- Back-Up Slides
Introduction

- New challenges exist for substantiating Government security investments:
  - Heightened interest in evaluating all significant Government investments as commercial industry would

- Transforming to Service-Oriented Architecture (SOA) enabled information sharing comes with a security investment beyond legacy information assurance considerations

- Government currently uses risk assessment methods to drive information security investment options
  - Assesses likelihood that vulnerabilities will be exploited

- Return-on-Investment (ROI) analysis is an enriched approach for determining appropriate investment levels
SOA Information Security Challenges

- Web services implementation of SOA introduces specific challenges based on loose coupling between consumers and providers

  - Dynamic discovery: therefore, no a priori knowledge of all users
  - Service level concerns
  - Responsiveness to threat situations
  - Expanded certification and accreditation scope
  - More insightful access determination mechanisms, e.g., role to allow info sharing
Addressing SOA Security Challenges

- SOA security solutions consider:
  - Access control
  - Consumer identification and authentication
    - differentiation according to attributes/privileges
  - Inhibiting consumers from correlating service discovery with providers
  - Access policies and identity management
  - Protecting service providers from “bad actor” consumers
  - Client and service authentication via transport layer security (TLS) protocols
  - Continuous monitoring and auditing
  - C&A policy and process alignment with SOA provider and consumer security requirements
Different investment decision-making approaches yield different results

“We already do risk analysis. Why ROI?”

More traditional information security solution selection

Recommended information security solution selection

Risk Analysis
Types of risks to minimize:
• Disruption of operations/service
• Damage to assets
• Loss of life
• Loss of stakeholder confidence
• Failure to comply with regs

Describe information security solutions according to risk mitigation capability

Risk-driven solution

Describe information security solutions according to mitigation capabilities, costs, benefits, and solution uncertainties/risks

ROI Analysis

Robust solution

ROI analysis is not new. It is recommended, and often compulsory, for many types of Government investments. It is a more robust method for determining the scope of an information security solution given operating environment complexities, fiscal constraints and increased regulatory scrutiny.
Government Information Security Investment Decision-Making Challenges

- Government regulation compels information security investment

Likewise, Government regulation also compels application of ROI techniques to substantiate significant investments

- An informed information security investment analysis is challenging because it must typically be performed when there is:
  - Uncertainty that a security breach would actually result as a consequence of foregoing an investment opportunity
  - Uncertainty regarding the magnitude of potential economic, national security, safety, civil liberties, and mission impact of a security breach
  - Difficulty in monetizing (i.e., translating into units of currency) potential benefits associated with security threat reduction/avoidance
Government Application of ROI Principles

- Commercial industry ROI methods do not readily translate for Government application
  - An ROI calculation is performed to quantitatively assess financial measures of investment attractiveness
  - An ROI analysis includes an ROI calculation, as well as other quantitative and qualitative investment impact assessments

![Diagram showing the components of an ROI analysis: Quantitative Analysis, Qualitative Analysis, and their intersection Hybrid Analysis.]

- Government investment decisions are not exclusively made according to positive monetary return.
The full spectrum of costs, benefits, and risks are considered to ensure that valuable investment opportunities are not overlooked.

The monetizability of costs, benefits, and risks determines the types of assessment methods to apply within the ROI analysis.

- Investment costs and benefits can be easily monetized? (e.g., salvage value)
- Investment costs and benefits can be monetized, but not easily? (e.g., productivity)
- Investment impacts cannot be accurately expressed monetarily? (e.g., degree of regulatory compliance)

ROI Calculation Suite of Metrics
- Net Present Value (NPV)
- Payback Period
- Internal Rate of Return (IRR)
- Cost/Benefit Ratio

EXAMPLE DECISION ANALYTIC APPROACHES
- Project Scorecard
- Borda Voting
- Multi-Attribute Utility Theory
- Real Options Theory
- Balanced Scorecard
- Other

Qualitative Assessment
- List of priorities
- List of relative desirability
- Comparative customer satisfaction ratings
- Balanced Scorecard ratings
- Number of voters "for" and "against!"

(1) What are the social consequences?
(2) What are the strategic implications?
(3) What is the effect on employee morale?
(4) What are the political ramifications?
(5) Stoplight matrix of risk assessment

Investments Selection

Performance Management Planning

Performance Monitoring

Post-Investment Review

SOA Information Security ROI Analysis (1 of 3)
SOA Information Security ROI Analysis (2 of 3)

- Key steps when performing any Government information security ROI analysis:
  
  - **Step 1:** Estimate the probability that a security breach will occur should the investment not be undertaken.
  
  - **Step 2:** Estimate the magnitude of identified risks for each security vulnerability in terms of potential impact on stakeholders (e.g., taxpaying citizens).
  
  - **Step 3:** Prioritize risks to be mitigated through information security investment options based on consideration of risk probability and magnitude.
  
  - **Step 4:** Estimate the cost of developing/acquiring and implementing the security controls for the alternative options. Don’t forget to consider opportunity cost.
  
  - **Step 5:** Estimate the on-going cost to maintain the information security investment at the level of effectiveness required. Don’t forget to include undesirable side effects.
  
  - **Step 6:** Identify and evaluate the risks that the information security features, if funded, will not provide the security expected or required.
  
  - **Step 7:** Determine the expected (i.e., uncertainty-weighted) value of damage from the prioritized major risks. Assess the effectiveness of the proposed investment to mitigate risks.

Tailor these for SOA information security investments.

Approved for Public Release: Case # 08-0363
SOA Information Security ROI Analysis (3 of 3)

- An actionable SOA ROI analysis method requires:
  - An understanding of Government ROI analysis best practices and lessons learned
  - Tailoring to address value tradeoffs that are unique to SOA information security investment
- Many information security considerations for SOA are similar to those for non-SOA environments

- Some additional security features to consider, however, include:
  - Provide security across Trust Domains
  - Preserve interoperability will addressing major security integration points in the architecture
    - Allow integration with existing information assurance solutions, products, and policies
  - Customize security policies
  - Secure other infrastructure services within the SOA
    - For example, discovery, messaging, mediation, and services management
Trust Domain Example

Need to verify trustworthiness of new consumers in Trust Domain C

Investment Need

Trust Domain A
- Service Consumers
- Always Trust

Service Provider

Always Trust

Trust Domain B
- Service Consumers

Trust Domain C
- Service Consumers
- Always Trust

Investment Idea

Trust mechanism between Service Provider and Trust Domain C consumers

Investment Scope

- What is the extensiveness of the cross boundary solution needed?
- What are the requirements to
  - Accommodate interfaces with enterprise level services?
  - Interact with multiple trust brokers?
  - Engineer solutions in instances where a broker cannot be leveraged?

Multiple Solutions

Trust C Because B Trusts C Broker Vouches

OR

Use Trust Broker

ROI ANALYSIS TRADE-OFFS

COST
- Price
- Opportunity Cost
- Performance Degradation
- Upkeep
- Hidden Cost

BENEFIT
- Performance Quality
- Alignment with Outcomes
- Enhanced Trusted Relations
- Improved Business Opportunity
- Risk Reduction
- Regulatory Compliance

UNCERTAINTY
- Cost Uncertainty
- Technical Performance Uncertainty
- Schedule Uncertainty

Investment Decision:
Conclusions (1 of 2)

- Government organizations should consider applying ROI analysis for making information security investment decisions
  - ROI analysis is more robust and appropriate for Government investment decision-making than ROI calculation
- ROI analysis is equally valuable for investment selection and management decisions
- ROI analysis can be resource intensive
  - The negative ramifications of not carefully considering tangible and intangible costs, benefits, and investment risks should be balanced against the resources required to conduct, and periodically update an ROI analysis

“ROI Lite” can be achieved by:
1. Developing an initial full-blown ROI analysis,
2. Identifying key drivers (i.e., “leading indicators”) of ROI
3. Monitoring status of only the key drivers over time
   - Major variances would signal a need to revisit the full-blown ROI analysis
Conclusions (2 of 2)

- The ROI analysis process can be as valuable as the results
  - Provides a systematic thought model for considering:
    - What is important to protect
    - The types of threats that exist
    - What might be the business impact of security breaches
  - To avoid “gaming the system”, Governance must ensure a standardized ROI analysis process is applied consistently

- In applying ROI analysis for SOA information security investment decision-making:
  - Begin with an understanding of how ROI analysis should be applied for typical information security investments
  - The most significant cost implications are not typically reflected in the price tag for security features