Budgeting and ROI Calculation for Security Organizations

Moving from FUD to Funds

Presented By: Donald Brooks
Don.brooks@sanasecurity.com

Agenda

- Traditional Security Solution Acquisition
- Requirements for a New Acquisition Paradigm
- Funding for Security Organizations
- ROI Calculation
- Business Case and Budgeting Justification
- Conclusion

Traditional Security Solution Acquisition

How Vendors Sell to Us

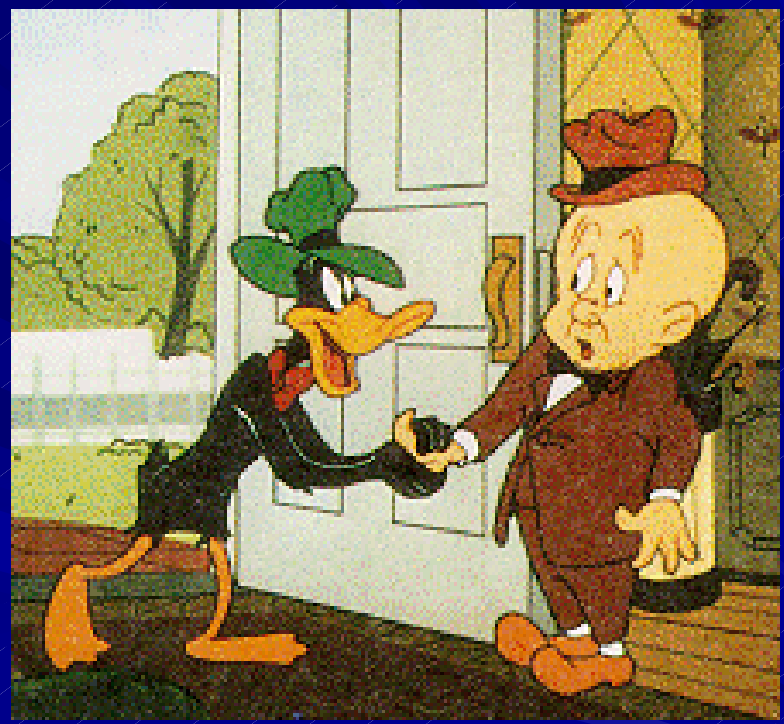
- Protection from Security Breaches
- Collecting Data About Intrusions
- Warn about Possible Vulnerabilities
- Prevent Successful Denial of Service Attacks

How We Sell Internally

- Past Security Issues and Events
- Damage or Loss of Data
- Damage to Reputation / Goodwill

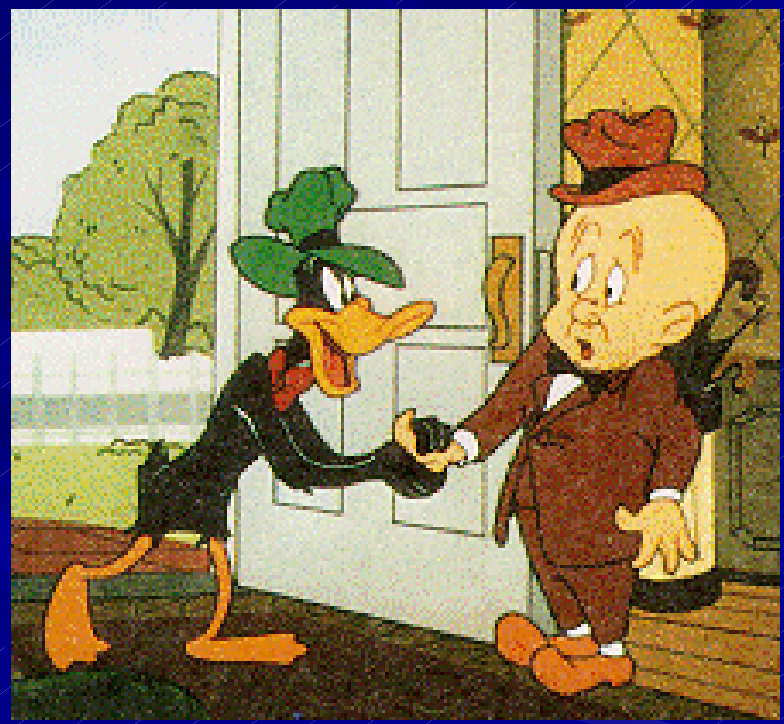
What Does This Mean?

- We Perpetuate the Fear, Uncertainty, and Doubt (FUD)
- We become insurance salespeople
- We Fail to Turn FUD into Funds



What the Money People Hear

- Though there is only a slight chance of anything happening, we need to buy insurance.
- This investment will not show ROI
- This investment will only show cost savings if we get attacked.



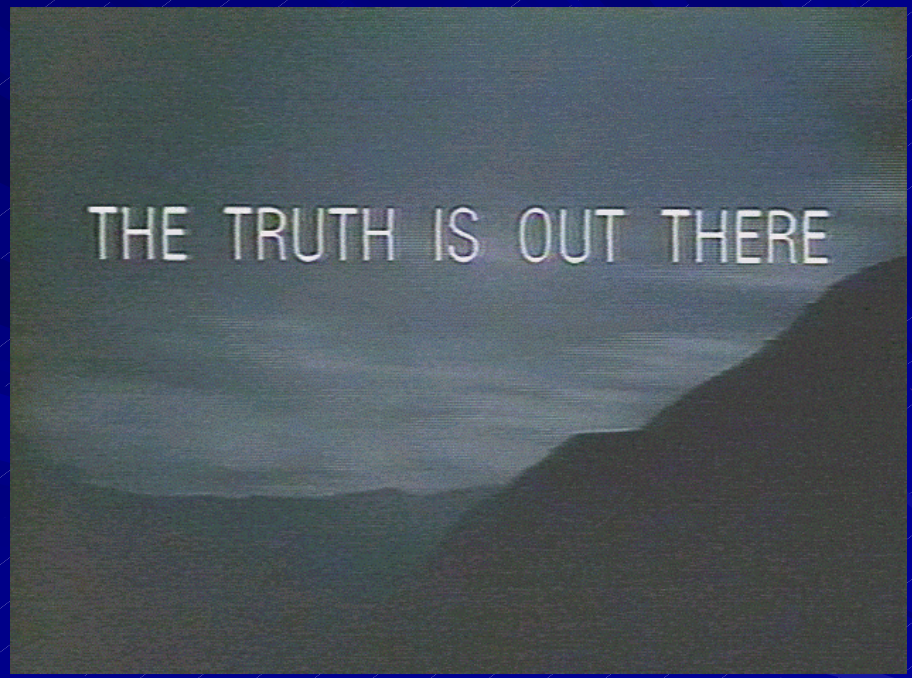
Requirements for a New Acquisition Paradigm

How Vendors Should Sell to Us

- How the Solution will Save my Organization Money
- How I can Show ROI with this Solution
- How the Information and Data that are Collected will Add Value
- How this Solution will Enable me to Work Smarter

How We Should Sell Internally

- Highlight True Costs, Including TCO
- Illustrate how Solutions will Impact the Security Organization's Budget
- Prove that the Solution will Enable the Security Organization to Better Support Strategic Business Objectives



What the Money People Will Hear

- Rather than a Cost Center, the Security Organization is a Business Enabler
- Security Solutions can Increase Productivity and Drive Down Costs thereby providing ROI
- Security Solutions are not strictly insurance

Funding for Security Organizations

Overview

- Insufficient funding is the most common finding in a root cause analysis of security incidents
- Lack of funding across the board
  - People
  - Process
  - Technology

Overview

- How is funding appropriated?
  - Funding as a reflection of perceived importance
  - As a function of regulatory / statutory compliance
  - Part of general IT budget
- For many organizations, information security is considered as only a cost center.

Overview

- How do we address the need for funding?
  - Compelling Events
  - Regulatory / Statutory requirements
  - Business Planning

ROI Calculation

ROI Basics

$$ROI = \frac{\text{Net Benefit}}{\text{Cost}} \times 100$$

<u>Example:</u>

If a project costs $10,000 and returned a net benefit of $5,000 in the first year, the ROI would be 50% (5,000/10,000 X 100)

Shortfalls in using basic ROI for security funding

- Does not account for opportunity costs
- Does not provide enough information to make informed decisions

Alternatives to basic ROI

- Quantitative Decision Analysis Approach
- Finance-Based Approach
  - Hedging
  - Opportunity Cost

The Soo Hoo Model

A Quantitative Decision Analysis Approach

- Decision Analysis approach
  - Based on work by Raiffa and Schlaifer (1961) and Howard (1966)
  - An approach that "dissects decision problems into constituent parts":
    - *Decisions* to be made
    - *Uncertainties* that make decisions difficult
    - *Preferences* used to value outcomes
  - 3 major advantages
    - Decision-driven
    - Uses probability theory to manage uncertainty
    - Uses influence diagrams as a common graphical language

Hedging

- Based on time-honored business risk-management strategies
- Investment Based
- Reduces budget variance and risk

Opportunity Cost

- Intangibles
- Cost of not doing business
- Unbudgeted costs

Opportunity Cost

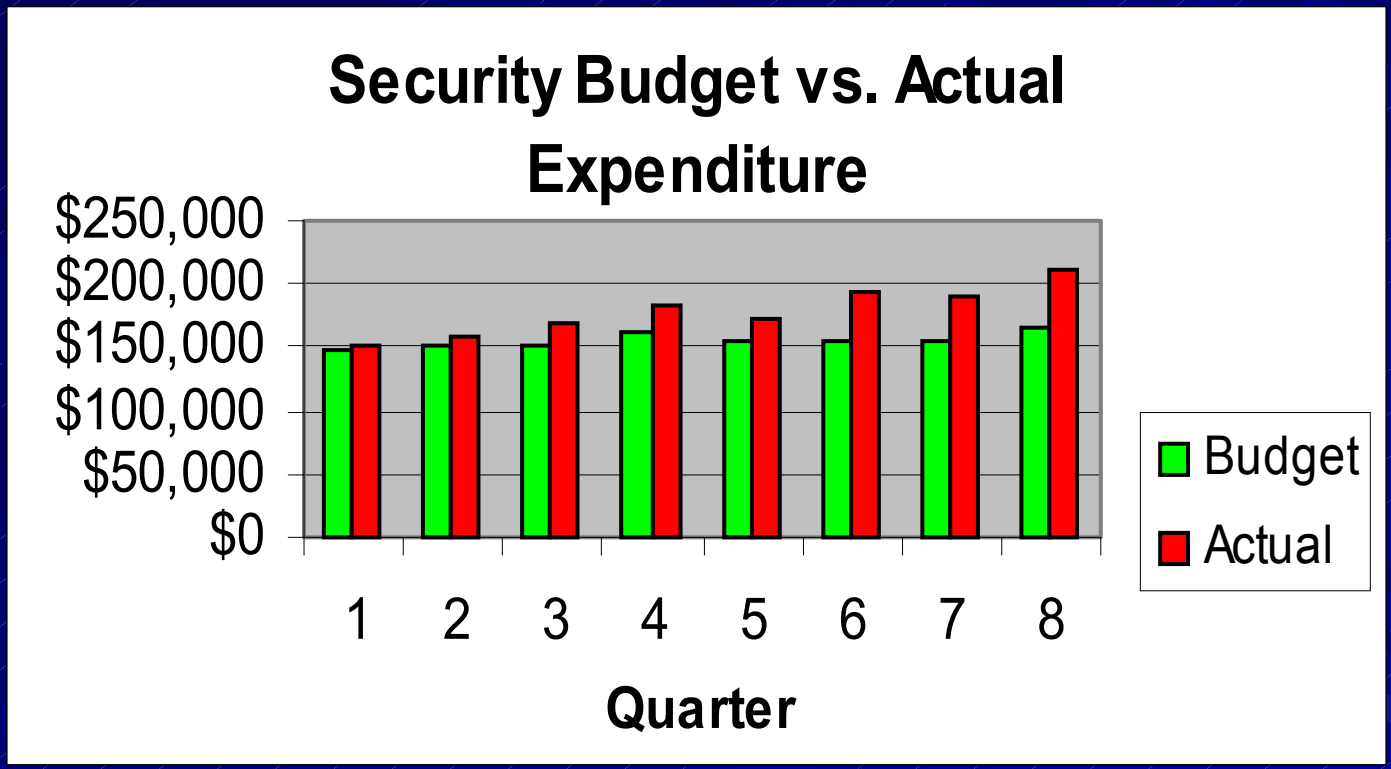
- Intangibles
- Cost of not doing business
- Costs of non-compliance
- Unbudgeted costs

Business Case and Budgeting Justification

Hedging – Step One

- Determine total dollars budgeted for information security
- Determine actual amount spent for information security

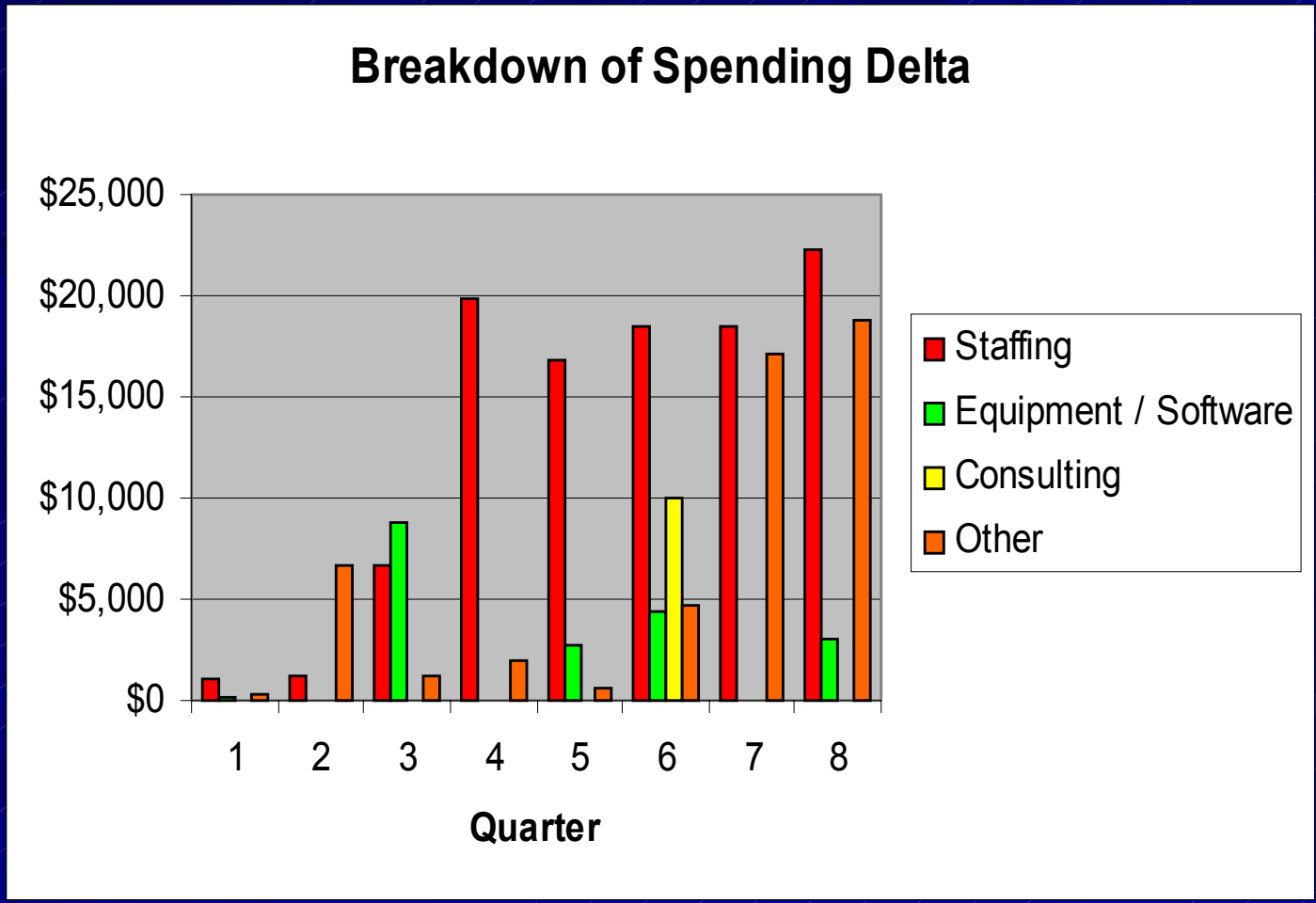
Hedging – Step Two



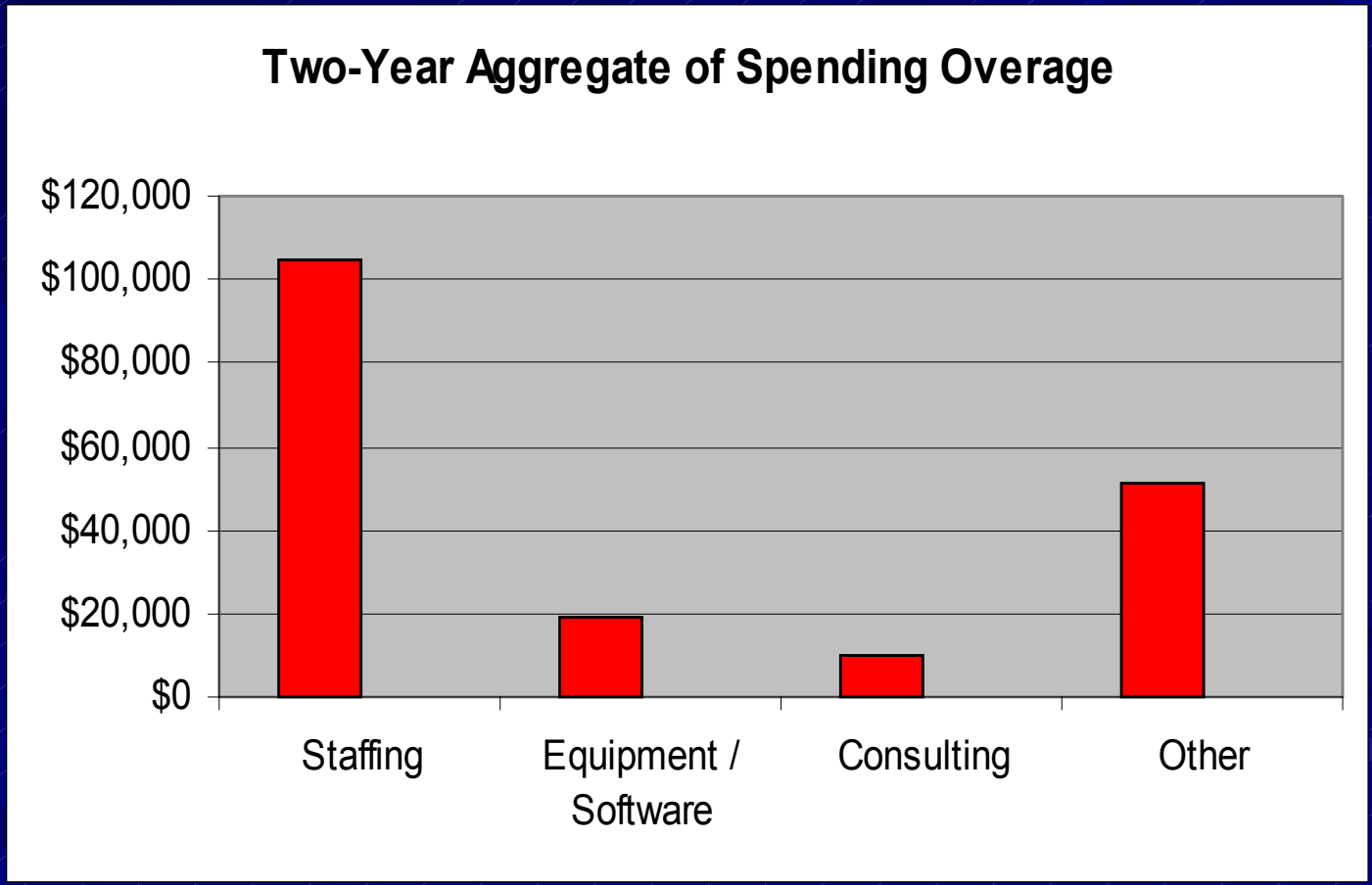
Hedging – Step Three

- Break down delta into categories
- Determine cost- and profit-center impacts of overage

Hedging – Step Four



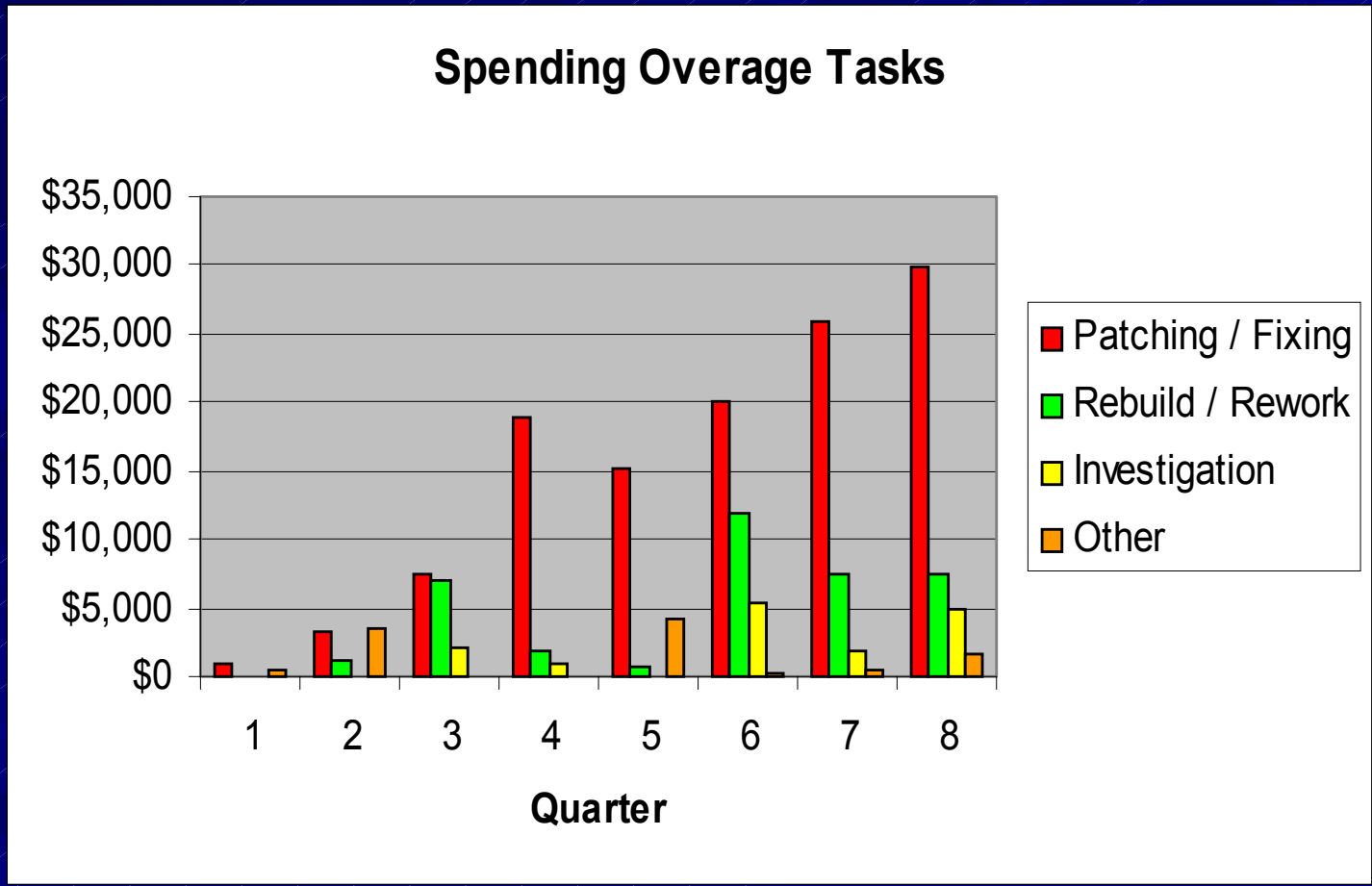
Hedging – Step Four



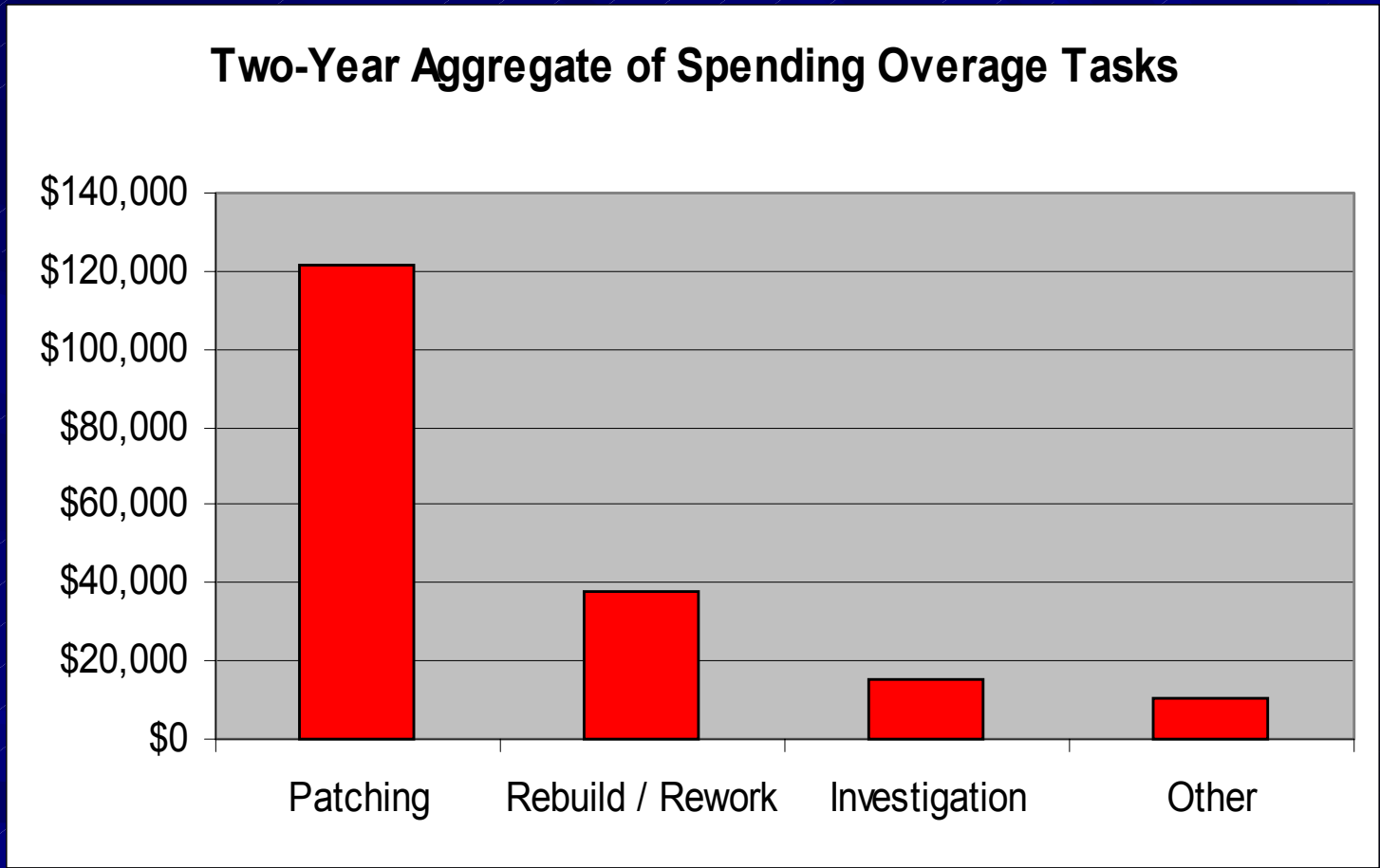
Hedging – Step Five

- Determine what caused spending delta by category
- Determine secondary and opportunity costs associated with any incidents

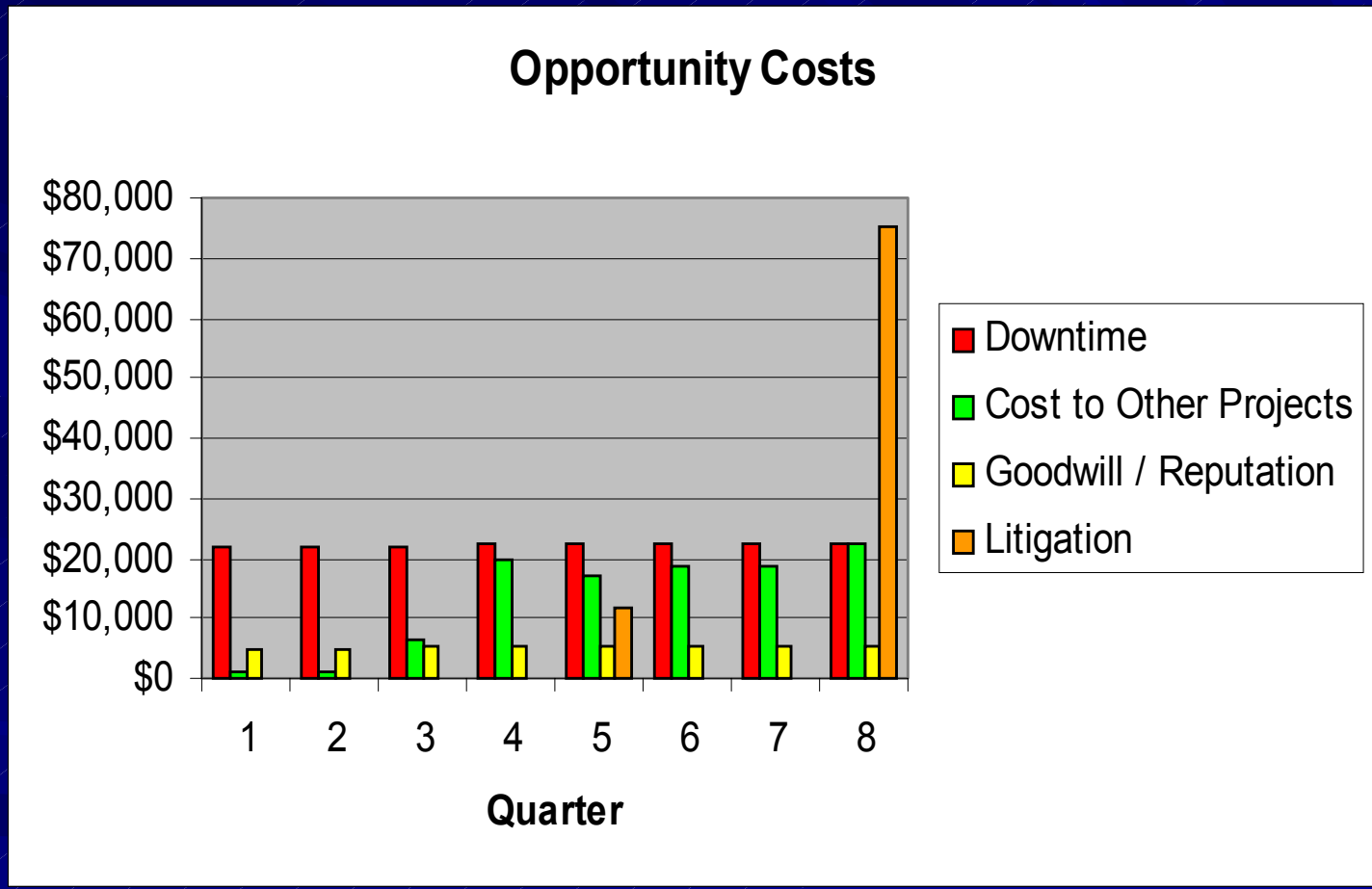
Hedging – Step Five



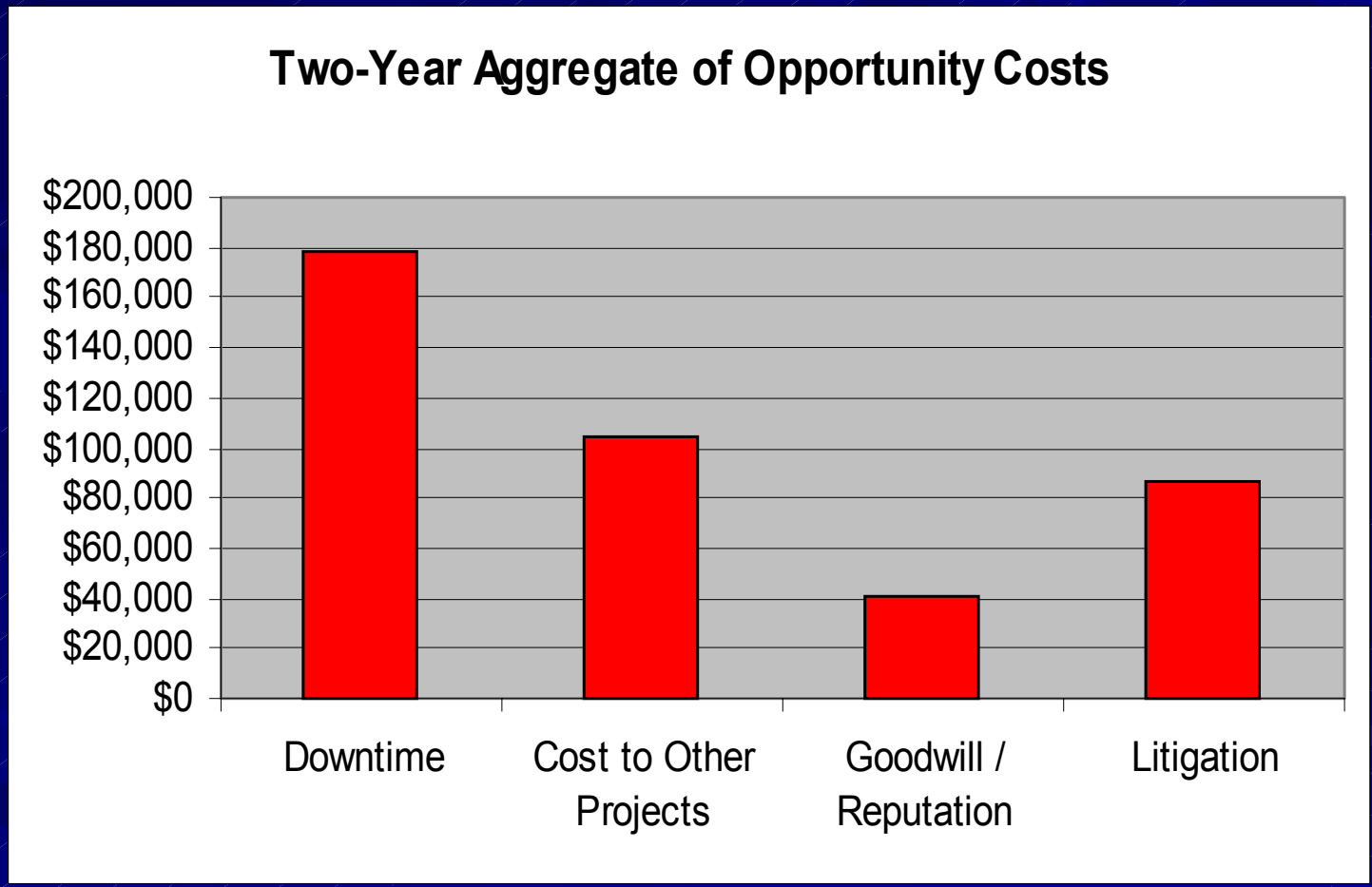
Hedging – Step Five



Hedging – Step Five



Hedging – Step Five



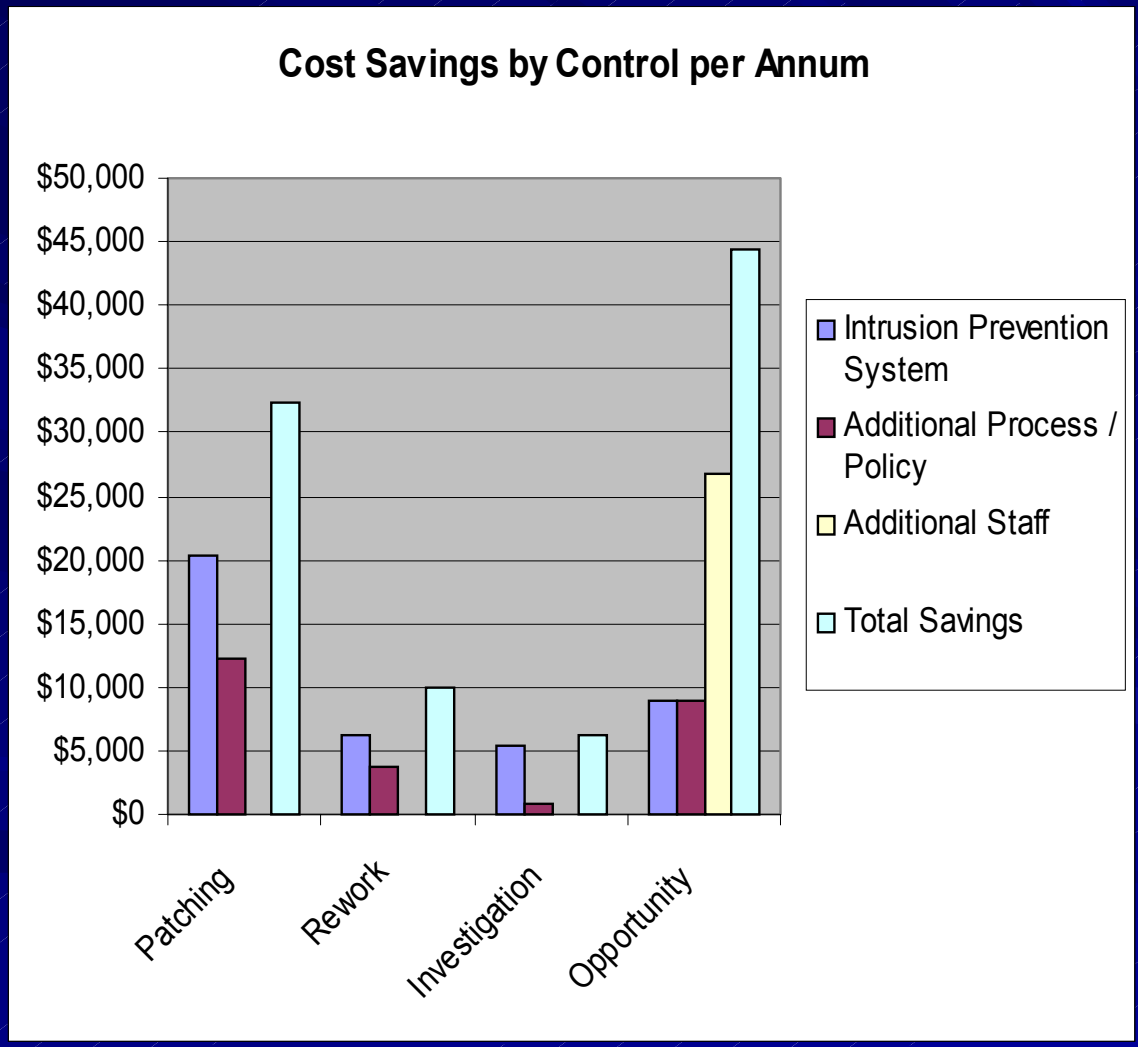
Hedging – Step Six

- Identify additional controls or resources that could mitigate risks and / or cut costs
- Plot cost reductions and risk mitigations so as to provide a basis for any funding requests

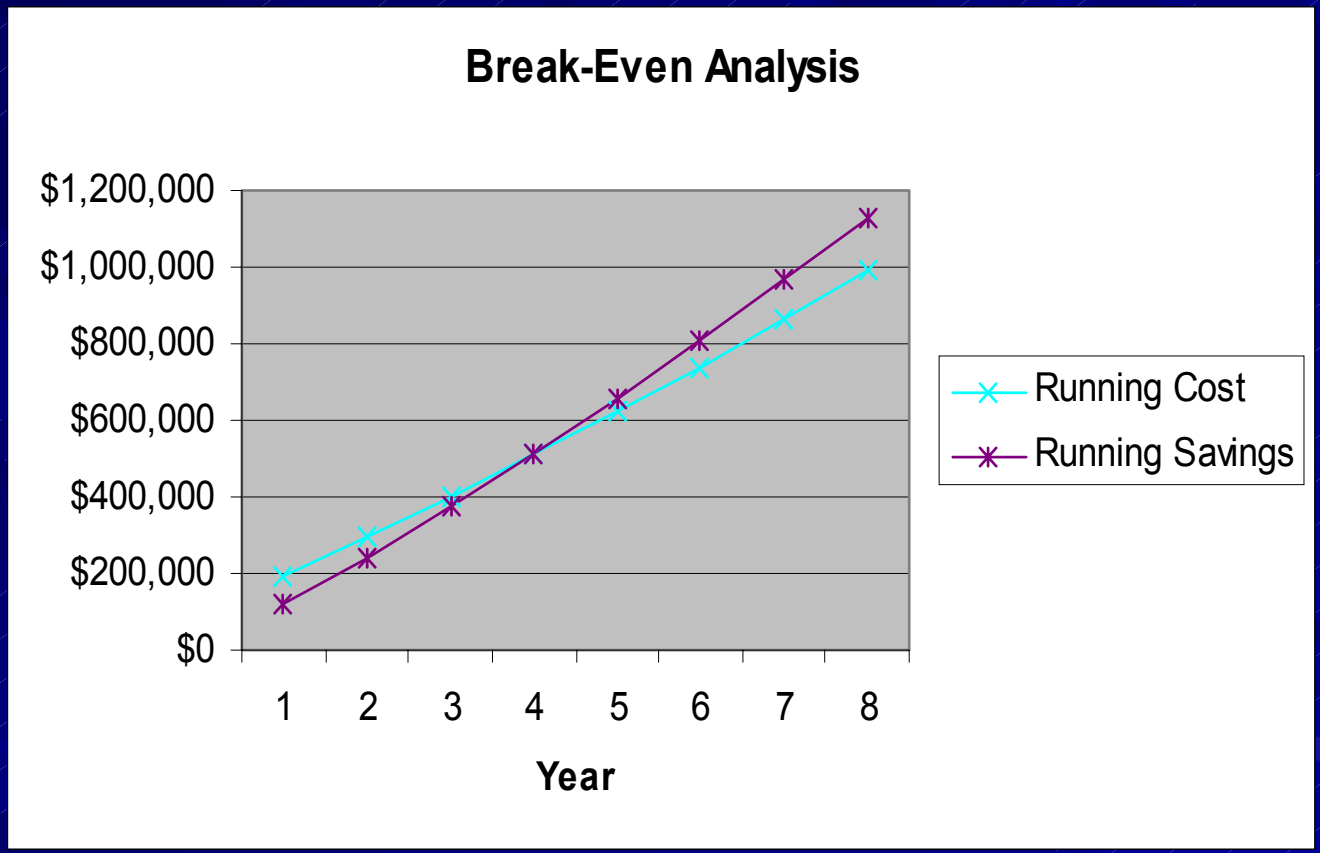
Hedging – Step Six

- **Additional Controls or Resources**
  - –Additional Security Policy and Process $40,000
  - –Additional Security Staff: $100,000 / FTE
  - –Intrusion Prevention System: $50,000–$100,000

Hedging – Step Six



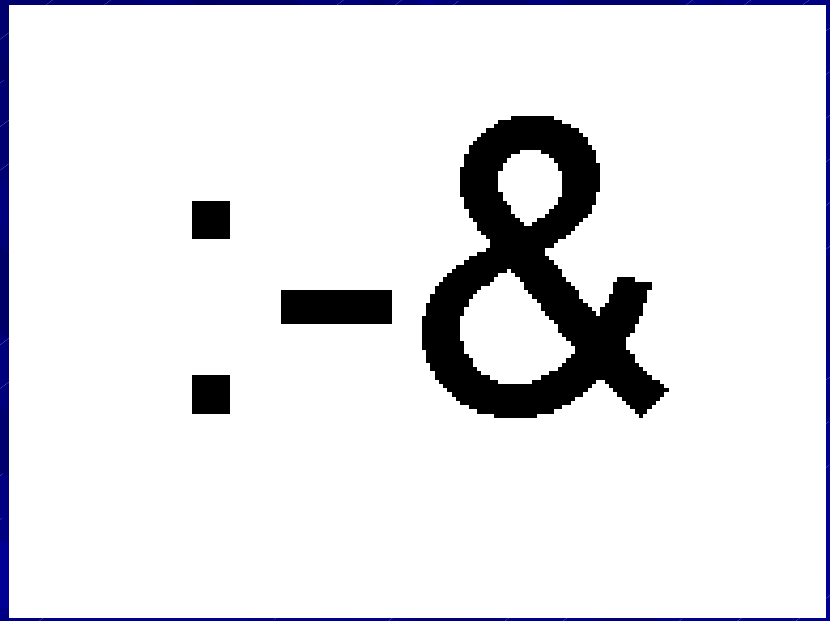
Hedging – Step Six



Conclusion

Learn the Language

- Risk and return vs. hubs and routers
- CIO – CFO – CEO
- Strategic vs. Tactical



Getting Started

- Books
  - The Successful Business Plan: Secrets and Strategies by Rhonda M. Abrams, Eugene Kleiner
  - Anatomy of a Business Plan: A Step-By-Step Guide to Starting Smart, Building the Business, and Securing Your Company's Future (Anatomy of a Business) by Linda Pinson, Jerry Jinnett
- Software
  - Business Plan Pro by Palo Alto Software
  - PlanView by Global Village
- Workshops / Education

Conclusion

- Plan your work, Work your plan
- ROI Alternatives
  - Decision Analysis
  - Hedging
  - Opportunity Costs
- Approach security as risk mitigator and not as a cost center

Budgeting and ROI Calculation for Security Organizations

Thank You

Don Brooks
don.brooks@sanasecurity.com