Justify the Return on Security Investments to Company Stakeholders

Crafting a quantifiable business case

The Current Situation…

- Emergency regulatory security changes are mandated
- Increased cyber/physical attacks on energy companies
- Increased security activity due to New York attacks; security funding spiked
- FY03/04 budget dollars under scrutiny [balloon shrinks]
- Corporate profitability requirements increasing
- Stock valuation under scrutiny
- Liability reaches from corporate to personal
- Energy industry is behind the technology curve yet Internet accessible to customers and vendors
- Energy industry has merged corporate/EMS-SCADA networks
- Security staff is not increasing at the same rate as IT growth & complexity
- Mid-sized companies have the smallest rate of increase

The Fundamentals..

- Understanding the Basics
  - Enterprise Objectives
  - Regulatory Mandates
  - Risk Analysis
  - Probability of Occurrence
  - Impact of Occurrence
  - Benefit to Enterprise
- How to Plan the Justification
  - Primary areas for Planning
  - Prioritize Risk Mitigation
  - Resource Availability
  - Comprehensive Plan of Attack
- Build the Business Case
  - Understand TCO, Timelines and Resource Requirements
  - Use Financial Metrics
  - Work with Finance - Capitalization
  - Articulate Impact – Piggyback
  - Meet Stakeholders Expectations
- Presentation of Business Plan
  - Get Finance buy-in & buy-off
  - Get Audit buy-in & buy-off
  - Speak to Stakeholders concerns
  - Meet Regulatory Objectives
  - Meet Strategic Security Objectives
  - Meet Tactical Security Objectives
  - Meet Audit Objectives
  - Set Foundational Direction for Strategic Objectives

Defining ROI and ROSI

- **Return on Investment (Return on Invested Capital)**
  - A measure of company's performance
    - Finite: Total capital divided into company's income
  - Sometimes equated with Return on Assets
  - Normally defined by the business as an '***incremental gain on an action***'
  - Three ways to increase ROI
    - Minimize costs
    - Maximize returns
    - Accelerate the timing of returns

Defining ROI and ROSI

- **Return on Security Investment**
  - Normally defined as the value of loss deference/reduction to dollars invested on security enhancements
    - Indefinite [having no exact limits]
  - Some security investments do have specific ROI
    - Provisioning users
    - Corporate insurance
  - Also defined as an ‘incremental gain on an action’
  - Four ways to increase ROSI
    - Minimize/eliminate operational losses
    - Minimize investment
    - Maximize positive returns (where ROI applies)
    - Accelerate the timing of returns

Understand the Basics

- **Enterprise Objectives for Security**
  - Obtain Blueprint documents from CTO/CIO to understand 5 year plan for technology growth in hardware/software/network
- **Regulatory Mandates**
  - Contact Compliance, Legal and industry groups to understand immediate and short-term/long-term regulatory requirements [FERC SMD, ISO standards]
- **Risk Analysis**
  - Understand your risks in cyber/physical security, disaster recovery/business continuation, and compliance to data protection/data sharing regulations
  - Quantify the impacts wherever possible; per incident, per potential loss
- **Probability of Occurrence**
  - Be realistic; use % for impact modifier
  - Pull industry trend information; poll federal/industry alliances; previous internal loss
- **Impact of Occurrence**
  - Be realistic; compute hard dollar impacts, estimate soft dollar based on real industry losses/settlements/pay-outs; poll industry vendors
- **Benefit to Enterprise**
  - Avoidance is one benefit but weak justification for getting approved funds
  - Tie to hard dollar savings/loss reduction – PIGGYBACK projects
  - Make sure your approved project has hooks set for the next project(s)
  - CREATE YOUR COMPREHENSIVE PLAN OF ATTACK FOR FUNDING

How to Plan the Justification

- **Three primary areas for security and DR/BCP planning**
  - **Prevention**
    - Preventing intrusion past the cyber/physical walls of the enterprise [draw-bridge up]
  - **Detection**
    - Ability to detect those that are attempting to mis-use corporate assets from the inside [outsiders and insiders alike]
  - **Reaction**
    - Incident Response (IR) capabilities have to be predetermined to be effective; point-in-time IR wastes time, money, resources and increases exposure

- **Prioritize Risk Mitigation – build a Risk Picture**
  - **Rank your identified risks based on the following**
    - Criticality [severity of impact – operational or monetary]
    - Cost to mitigate risk [total cost of ownership]
    - Duration of project [use 3 month increments for deliverables]
    - Determine a relative value for each risk

- **Resource Availability**
  - Be realistic: what staff/contractors/staff augmentation are you going to need to succeed?
  - What concurrent project implementations are going to use the same resource/funding pool?
  - Timing industry resources to augment your internal/external timelines
  - Existing budget cycle or have to plan for the next fiscal year? Federal mandates**?**

Comprehensive Plan of Attack

- **Use your Risk Picture as the source of project determination**
  - Stratify risks into Strategic & Tactical [Critical, High, Medium, Low]
  - Include Audit in the evaluation process to determine what has been previously identified; Audit can be your best friend
  - Present Risk Picture to appropriate management to educate, lobby and to obtain acceptance of credible risk
- **Plan your projects so they create a foundation on which all other plans can rest**
  - Plan Strategic projects in conjunction to Tactical
  - Go after funding of core 'P-D-R' projects to build the technological solution/foundation
  - Make sure that you have the staffing/industry resources available to succeed within the timeframes that are required
- **How to prove that your projects will benefit the enterprise**
  - Succeed on early project implementations – use qualified project managers from your PMO - don't start what you can't finish – ensure a win-win
  - **MOST SECURITY PROJECT COSTS ARE RECOVERABLE THROUGH CAPITALIZATION – Know the financial requirements!**

Build the Business Case

- **Understand TCO**
  - Total Cost of Ownership – use Finance to assist; plan across next 5 fiscal years [understand where you can cut if necessary]
  - Be realistic – most security expenses/investments are OMAG after the first year [CAPITALIZE wherever possible]
- **Timelines and Resource Requirements**
  - Articulate inter-dependencies between security initiatives
  - Speak to the large plan; cross-utilize resources
  - Use Federal deadlines/compliance requirements to your advantage
  - Make contact with industry firms early to determine resource availability
  - **Try to MINIMIZE EXPENSES** [save up for future battles]
- **Use Financial Metrics**
  - Build metrics that can reflect your project progress, incident response, intrusion detection, cost avoidance: Always be ready to estimate financial cost avoidance from a deterred incident [proof is in the pudding]
  - Provides immediate feedback of success and hardened evidence of ROSI for future projects/enhancements

Build the Business Case (cont')

Work with Finance – Capitalize where you can

- Capitalize, capitalize, capitalize: money recovered is reflected differently on the books
- Be very careful in your understanding and categorization of capitalization

- **Articulate Impact – Piggyback**
  - You have to be able to articulate what the umbrella benefit is, what the specific impact potential might be, and the specific benefits of each project
  - Piggyback related projects to provide 'value-added' benefit where there is a standardized ROI for a security-related technology investment

- **Meet Stakeholders Expectations**
  - Write the narrative to the expectations of your project stakeholders
  - Know what they need to accomplish within their purview [financial, organizational, resource management, bonus structure, etc]

Get Stakeholder Attention

- **Who is the Owner of the security issue being addressed?**
  - What is the highest level of management impacted: these are your project Stakeholders and Champions
- **Can you articulate the risk and impact?**
  - Do your homework; get seed monies to bring in the experts for risk evaluation
  - Build your plan of attack to mitigate ALL risks, not just the one at hand
  - Ensure that your plans match the enterprise/Stakeholder plans
  - Capitalize your projects – present the recovery as justification
- **Risk Mitigation vs. Risk Acceptance**
  - Present ALL options
  - Require sign-off for risk acceptance
  - Encourages understanding of the risk and enables risk mitigation
- **Keep Stakeholders informed**
  - Have a comprehensive Security/DR/BCP framework
  - Report key metrics on a regular basis
  - Know who your Champions are and meet their needs

Presentation of Business Plan

- **Get Finance buy-in & buy-off**
  - Work with your Finance area to ensure the Investment Committee requirements are met
  - Understand what is normally expected by the Executive Management approval boards – Meet those requirements
  - Request Finance to informally approve the content prior to any presentation or business case delivery

- **Get Audit buy-in & buy-off**
  - Work with Audit on the post-risk analysis review to provide credible and concrete requirements that need to be met
  - Obtain an Audit representative that knows technology and the inherent risks – Audit can be your best friend
  - Obtain an informal agreement that the stated project scope will meet the risk mitigation requirements for the stated risk

- **Speak to Stakeholders concerns**
  - Research what is on the table for Investment Committee approval to understand where your business case fits in – LOBBY ahead of time
  - Present the benefit to the enterprise, the specific organizational units involved, the Strategic and Tactical steps being taken
  - Present the Financial material in support of the investment
  - Present the Audit material in support of the investment for the risk mitigation project

Presentation of Business Plan (cont')

- **Meet Regulatory Objectives**
  - Build in all regulatory requirements that are fully, or partially, met by your project
  - Project plans have to be realistic and meet the federal/state regulatory requirement timeframes
  - Build project metrics to provide a reporting measure to the Board, Management and Audit groups

- **Meet Strategic Security Objectives**
  - Articulate the overall security plan for the organization and how this project fits into the cyber/physical, DR/BCP Strategic objectives of the company
  - Define the core benefits that lend to the strategic direction
  - Each project needs to be tied to at least one of the security objectives identified in the Risk Picture

- **Meet Tactical Security Objectives**
  - Each project will share resources and funding pools
  - Define where economies of scale are utilized and the impact of delay
  - Each project needs to be tied to at least one of the security objectives identified in the Risk Picture and/or Regulatory mandates
  - The results of the project must meet the requirements of the technology Blueprint

Presentation of Business Plan (cont')

- **Meet Audit Objectives**
  - Audit has specific areas of concern today
    - Know them and meet them
  - Utilize the existing Audit relationship to provide credibility and appropriate urgency for initiating security projects
  - Understand the criteria for success that Audit uses for the concerns being addressed
  - Meet the criteria
    - Use Audit approved metrics
    - Require periodic Audit review [not just at the project end]

- **Set Foundational Direction for Strategic Objectives**
  - Ensure that you have provided the Investment Committee with a clear understanding of how your project adds value to:
    - Enterprise Strategic Objectives
    - Security Strategic Objectives

Justifying Security Investment

Security investment is hard to quantify.

The need is known, the impact is real, the justification ahead of time is difficult.

Use business defined ROI as a core and use realistic extrapolations to determine impact, loss deference, of investing in appropriate security.

Resources

- FERC – Federal Energy Regulatory Commission
  - www.ferc.fed.us
- NERC – North American Electric Reliability Council
  - www.nerc.com
- ES-ISAC – Energy Sector Information Sharing & Analysis Center
  - www.esisac.com
- NIPC – National Infrastructure Protection Center
  - www.nipc.gov
- CIAO – Critical Infrastructure Assurance Office
  - www.ciao.gov
- InfraGard
  - www.infragard.net
- ISSA – Information Systems Security Association
  - www.issa.org
- SANS Institute – SysAdmin, Audit, Network & Security Institute
  - www.sans.org

Questions?

L Chris N Shepherd

chris.shepherd@icctcorp.com
http://www.icctcorp.com
877.905.0209