



Washington Group International

Integrated Engineering, Construction, and Management Solutions

Making the Business Case for IT Security

Gary Bronson

Director, IT Enterprise Operations

November, 2003

Agenda

- ◆ What We Learned from our Security Conference in May, 2003
- ◆ Structuring the “Business Case”
- ◆ WGINT Business Case Review
- ◆ Summary



Learning's From our Security Conference



Key Participants

Peter Coffee, Technical Writer, eWeek

Kathleen Roberts, VP, AT&T

Ray Wagner, PhD, Gartner's Security Strategies Group

Dwight Pond, General Manager, ITG

Ira Winkler, Chief Security Strategist, HP

Brett Arsenault, Strategic Technology Director, Microsoft

William Vaas, VP, Sun Microsystems

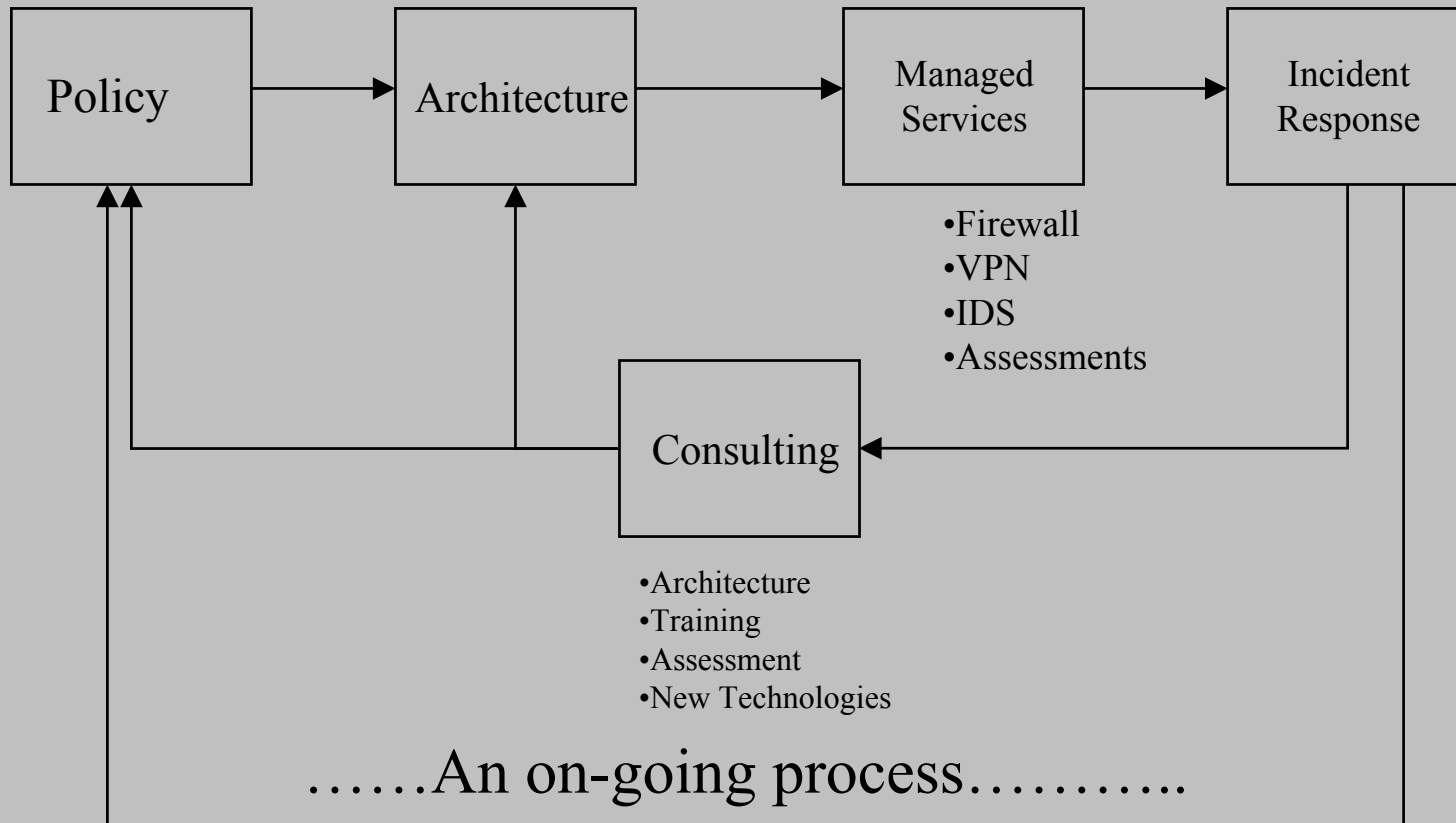
Deborah Frincke, PhD, Professor University of Idaho

Gary Bronson, Director IT Operations, Washington Group Int.

Key Learning's

- ◆ Not just an IT issue
 - A bottom-up approach for almost any business process doesn't work and has little chance of success
- ◆ Security should be built in, not Bolted On!
- ◆ Defense in Depth
 - No single silver bullet
 - Mitigate... don't try and eliminate Risk!
- ◆ Security is a concern and a high priority, however, still considered complicated and expensive
 - 90% of security issues can be addressed by focusing on the basics
 - Avoid a 'technology fix' and focus on what assets need to be protected and what is the value of those assets
 - Don't worry about the hype and buzzwords... Simplify!!
- ◆ Security is an on-going process...

A Lifecycle of Security



Dennis Treece, CSO MassPort

- ◆ Security professionals need metrics and tools to better justify the cost and value of information and physical security measures
- ◆ Despite increased attention to security following the Sept. 11 attacks, security operations must still compete for corporate resources.
- ◆ Security professionals need to be able to talk about security risks in quantifiable business terms that management understands
- ◆ Warning senior management about the ever-growing tide of threats and vulnerabilities only goes so far. After awhile security managers begin to sound like Chicken Little and executives stop listening.

The SKY IS FALLING!!!

- ◆ The Kansas state legislative auditor cracked over 60% of the passwords at the state's Health and Environment Department. Auditors used password cracking software to break more than 1,000 passwords, including several administrator's passwords.
- ◆ In a report released in October 2003, the auditor found the department's IT systems to be "poorly configured and infected with a large number of different viruses, worms and Trojan horses."
- ◆ In response to the auditors recommendations, the department hired FishNet Security Inc. of Kansas City, Mo., for a complete vulnerability assessment.

Vendors that Participated in the Conference





Format of the Business Case



Defining A Business Case

- ◆ The Business Case forms the foundation for any proposed venture or project.
- ◆ It establishes the need, justification and proposed alternatives to resolving a business issue or strategic objective.
- ◆ The Business Case will discuss the alternative solutions explored and the conclusions reached.
- ◆ It will identify the risks of each alternative and establish the economic justification for the proposed course of action.
- ◆ In addition, it will project future returns to justify the cost of the project or venture.

Defining A Business Case

- ◆ The Business Case is a document which should be updated at key milestones during the project's lifecycle.
- ◆ Where discrepancy is found, the Business Case should be updated to reflect the current circumstances
- ◆ A Business Case is written by 'the business' or commercial side of the organization, **but** often with strong support and input from the IT section / department to aid with the (inevitable) technical aspects of the proposal.

Defining A Business Case

- ◆ Today's best-of-breed business cases share three elements:
 - They are complete
 - They have accountable results
 - They ensure a realization of benefits.
- ◆ The point of a business case is to help a company realize value from its investments. Whether in IT or elsewhere in the company, that's possible only if the plan is realistic, workable, and comprehensive.
- ◆ Shareholders don't want a great business case--they want the benefits described in the case.

<http://www.optimizemag.com/issue/003/roi.htm>

Tips From Cert (www.cert.org)

- ◆ Present in meaningful terms for the Audience
 - Business objectives, market share, customer satisfaction, privacy and competition
- ◆ Show you care as much about the Business as you want the Business to care about Security
- ◆ Demonstrate the mitigation of risk on particular assets
 - Note: Unacceptable security practices may still be an acceptable business risk!
- ◆ Compare your organization with others in your market segment
- ◆ Involve key stakeholders in this process and make your business case using a structured approach

CSO Online

- ◆ **Return On Security Investment:** Risk economics that paints a picture of your organization's attitude toward security.
 - What level of risk is the enterprise comfortable with?
 - How does the company prioritize its limited resources?
 - Is technology or awareness more valuable as a tool?
- ◆ **Step 1: Rethink Assumptions**
 - Precision is not the goal—Accuracy... not precision
 - The Dogmatic I.T. mind-set must be eliminated
- ◆ **Step 2: Do the Legwork**
 - Find and use existing data
 - Know thyself
 - Calculate conservatively
 - Know Your Audience
- ◆ **Step 3: Do the Math**
 - Incident Cost x Probability of Incident
 - $ROSI = Savings - Mitigation Costs$

Business Case for IDS - SANS

1. Why should you deploy an IDS?
2. What is the Return on Investment (ROI) for an IDS?
3. What it will cost to deploy the IDS?
4. What cost savings/avoidance will be made possible by deploying the IDS (Where might you save money that is being spent today/prevent money from having to be spent?)?

www.sans.org/resources/idfaq/business_case_ids.php



WGINT Case Study



WGINT: Case Study (What Not to Do!)

- ◆ Step 0: Fall 2001– Submit request to CIO for Security Manager... denied...
- ◆ Step 1: Vulnerability Assessment (Oct, 2002)
 - Orchestrated by CIO
 - Didn't coordinate with Senior IT Operations Management
 - Planned a Leadership Conference on the other side of the country during the Assessment
 - Used an unknown vendor
 - ✘ Coincidentally: 1 month after assessment a DoS occurred...the night before the vendor was hitting our system—said they had nothing to do with the DoS
 - Gave modem numbers for every modem across the country
 - Escorted into the premises and allowed to do vulnerability assessments during a Payroll run without a defined scope of testing
- ◆ Step 2: Distributing the Results
 - Fed ALL information during the process to the CFO—including hype from the vendor—without analyzing the information
 - Distributed UNIX System information to Network Ops

WGINT: Case Study (What Not to Do!)

- ◆ Step 3: The Sky Is Falling!
 - CIO Created a sense of fear in the environment
 - CIO over reacted– most of the high priority issues were resolved within a few weeks: Modems left on, Simple Passwords, Default Passwords, Test Systems accessible, Community Strings
 - Office of the Chair/Audit Committee directly involved
- ◆ Step 4: Create a Massive Project to address all layers of security
 - Go after large dollar amounts
 - Establish high expectations
- ◆ Step 5: Spend 9 months trying to get approval for the Massive Project
- ◆ Step 6: Aug, 2003 CIO asked to leave—Announcement of outsourcing ALL of IT Operations:
 - Save Money
 - Solve All our Security Problems

Summary

- ◆ Be Realistic
- ◆ Break down efforts into small manageable projects
- ◆ OK to ask for outside Help
- ◆ Don't wait to do the right thing!
- ◆ A Security Focus should be built into procedures at all levels: Users, Sysadm, Functional Management, Executive Management
- ◆ Don't spend a lot of money in one area and ignore the others...

– Parable of the Mailbox:



Reference Material

- ◆ “Security Best Practices Will Do Most to Foil Cyberterrorsts” Paul Schmitz, John S. Mazur, Rich Moquill (Gartner, 3 Oct 2002)
- ◆ “Management Alert: Beware of Invalid Assumptions” John Girard (Gartner, 4 Sept 2002)
- ◆ “Public Companies Should Prepare to Report on Their Security Readiness”, John Pescatore (Gartner, 14 October 2003)
- ◆ “Executive Summary: Information Security—How Much Is Enough?”, Richard Hunter (Gartner, April 2003)
- ◆ “Defining a New Framework”, www.compete.org/cs/
- ◆ www.sans.org
- ◆ www.cert.org
- ◆ “Enterprise Security *The Manager’s Defense Guide*”, David Leon Clark