Holistic Security

A Discussion of Risk Analysis & Strategic Initiatives

by: Benjamin Tomhave

Agenda, Part I

- Introduction
  - Rules of Engagement
  - Legalese
  - About Me
- Old School IT
- N3w Sk3w1 IT
- What is “Holistic Security”?

Agenda, Part II

- The Challenge: IT Alignment
- The Solution: Holistic, Strategic Security
- Hey, BRRAU
- Sample cases of **BAD** projects
- Sample cases of **GOOD** projects

Rules of Engagement

- Cell phones and pagers:
  - You have a job, feel free to leave them on.
  - Please keep them in reach to stop tone quickly.
  - Please move outside the room immediately when taking a call.
- Q&A:
  - Please ask questions!
  - Please make corrections!
  - I'm a consultant, not a supernatural entity – the possibility exists that I might be wrong! ☺

Legalese

- **Disclaimer:** The views, opinions, content, techniques, etc., included in this presentation do not necessarily represent those of my employer.

- **Copyright:** Unless otherwise stated, all opinions, slides, content, images, techniques, etc., included in this presentation are the Intellectual Property of Benjamin Tomhave.

About Me

- Pre-1994: Desktop weenie; introduced to UNIX; programming in BASIC, PASCAL, C
- 1994: UNIX and Network Admin – Ever supported academia?
- 1996-1998: Freelance, random project, internships, co-ops
- 1998: INS (no, not **the** INS)
- 1999: Ernst & Young
- 2000: BORN

A Quote

- “Interoperability is **NOT** a technology issue – it is a management issue. Next question please.”
  - General Powell (ret.), at Interop ‘99

Old School IT

- Centralized computing
- Centralized administration
- Ad hoc solutions
- Firefighting approach
- IT dictates to the business
- IT holds lots of power
- Security is the absolute last thought, if at all

N3w Sk3w1 IT

- Distributed computing
- Cost Constraints, Financial Implications
- HA Requirements
- Distributed or Centralized support
- Standardization
- Globalization
- Business is beginning to “understand” IT
- Reduced implementation schedules

What is “Holistic Security”?

- Comprehensive
  - Corporate Security Policy
  - Business Continuity Plan
  - Incident Response and Handling
- Managed
  - Better design
  - Cost-effective solutions
  - Not piecemeal! Less firefighting!
- IT Supports the Business, rather than Controlling it

The Challenge: IT Alignment

Traditional Approach

- Business states need
- IT provides solution, often redefining need based on tech known
- Business adapts, changing vision
- IT implements, business approves, some QA
- Don't like it? Too bad!

Contemporary Approach

- Business states need
- IT co-develops solution with BAs
- IT adapts to the business vision
- Strong design up front, followed by managed implementation w/ QA
- Don't like it? Fix it!

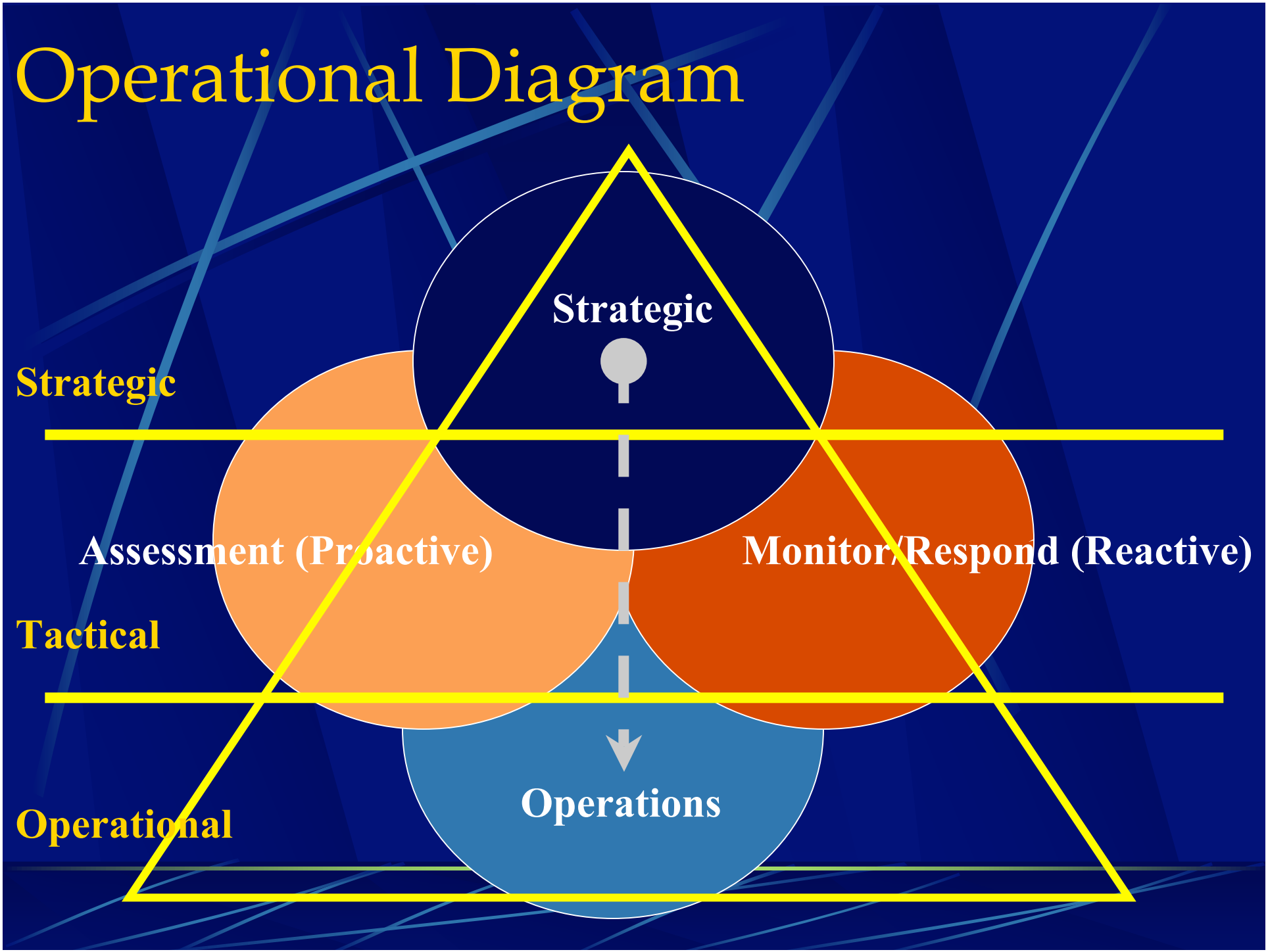
The Challenge: IT Alignment

- So, what's the problem?
  - IT still traditional, Business is contemporary
- How are "we" doing?
  - Depends on who's running your IT
- Who needs to change?
  - IT does!

The Solution: Holistic, Strategic Security

- Comprehensive, Business Solutions
- Strategic Initiatives = High-level buy-in
- Why A Strategic Approach?
  - Operational Diagram

Operational Diagram



Hey, BRRAU

- Basement Research Risk Attribute Utility
- http://www.basementresearch.net/
- Content will be coming to the site in the future.
- General utility – not just apropos to security!

©Risk = A^V x P^C x T^F

A^V is "Asset Value"*

P^C is "Probability of Compromise"

T^F is "Threat Frequency"

*Asset Value is fixed or increasing.

©Risk = A^V x P^C x T^F

P^C = Probability of Compromise

1) Software Defects
   - Bugs and Patches
   - System Maintenance
   - Discovery
2) Configuration Errors/Weaknesses
   - Inadequate filters
   - Weak firewall rules
   - Inadequate OS configuration

$^{©}Risk = A^{V} \times P^{C} \times T^{F}$

P^{C} = Probability of Compromise

- Mitigation Methods
  - Network Assessment (non-/intrusive)
  - Audit/Compliance
  - Development Code Review
  - Critical Design Review
  - Maintenance Procedures Review
  - Etc…

©Risk = A^V x P^C x T^F

T^F = Threat Frequency ("human factor")

1) Social Engineering
2) Human Error
3) Disgruntled Employees

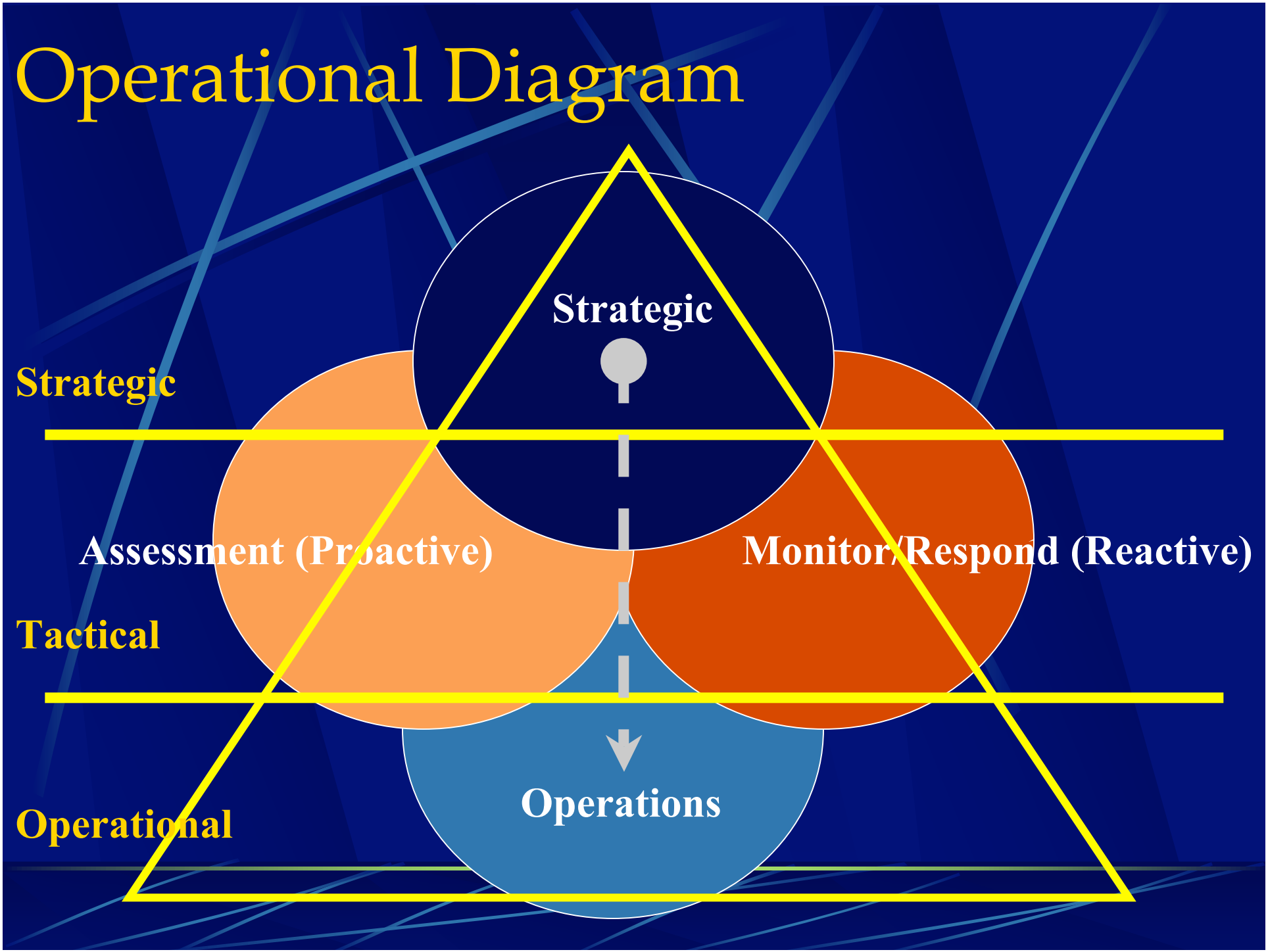
- 80-90% of security incidents originate from inside the firewall/organization
- Very difficult to measure & defense

©Risk = A^V x P^C x T^F

T^F = Threat Frequency ("human factor")

- **Mitigation Methods**
  - **Corporate Security Policy**
  - **Business Continuity Plan**
  - **Policy Enforcement & Buy-in**
  - **Intrusion Detection & Network Management Systems**
  - **Single Sign-On & Directory Services**
  - **Education & Awareness**

Operational Diagram



Sample cases of BAD projects

- Major retailer #1, failed eCommerce site
- Major retailer #2, failed eCommerce site
- Hershey & IBM: The SAP Disaster

Sample cases of GOOD projects

- Local data reporting center
- Original Amazon.com
- W2K Solutions Management
- Other misc:
  - Banks
  - Online trading
  - “Do it right the first time.”

Questions / Discussion

Contact Information

Benjamin Tomhave, BORN consultant
benjamin.tomhave@born.com

American Falcon, freelance security pundit
american_falcon@yahoo.com
http://falcon.cybersecret.com/