SearchFinancialSecurity.com
INFORMATION SECURITY
FINANCIAL
INFORMATION SECURITY DECISIONS

Managing an Information Security Program in a Difficult Market

Dealing with Trends and Facing Reality

Anish Bhimani

Major Trends 2008-2009

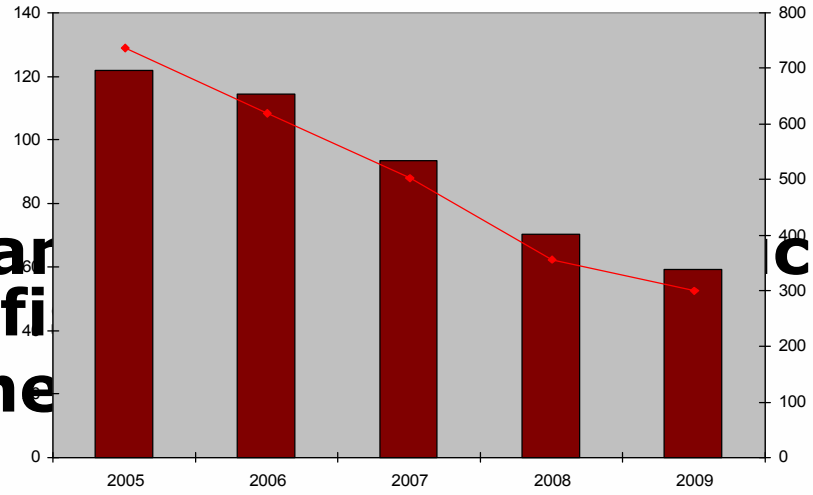
- **Increased Regulatory Scrutiny**
- **Increased focus of attacks on specific targets**
- **Increased media awareness about privacy and threats to reputational risk**
- **The "extended enterprise"**
- **The evolution of "security" into risk management**

Major Trends 2008-2009

- **Increased Regulatory Scrutiny**
- **Increased focus of attacks on specific targets**
- **Increased media awareness about privacy and threats to reputational risk**
- **The "extended enterprise"**
- **The evolution of "security" into risk management**
- ***…And a rapidly changing market and financial landscape***

A Dose of Reality

- Financial realities have changes
- Increasing push to rationalize IT spend



- How to balar ce risk with the need to be fi
- In good time

Striking the Right Balance

PRODUCTIVITY

- Efficient Operations
- Location Strategy
- Automation
- Investment Prioritization

QUALITY

- Service Delivery
- Instrumentation
- Customer/Channel Impact

CONTROLS

- Regulatory Compliance
- Privacy / Reputational Risk
- Identity & Access Management
- 3rd party risk / extended enterprise
- Linkage with Business Controls

Driving Productivity in IT Security

- **Overall security budgets are going down, but security investments are going up**
- **Greater spend does not necessarily equal more security**
- **Spend less on security without compromising controls**

Driving Productivity in IT Security

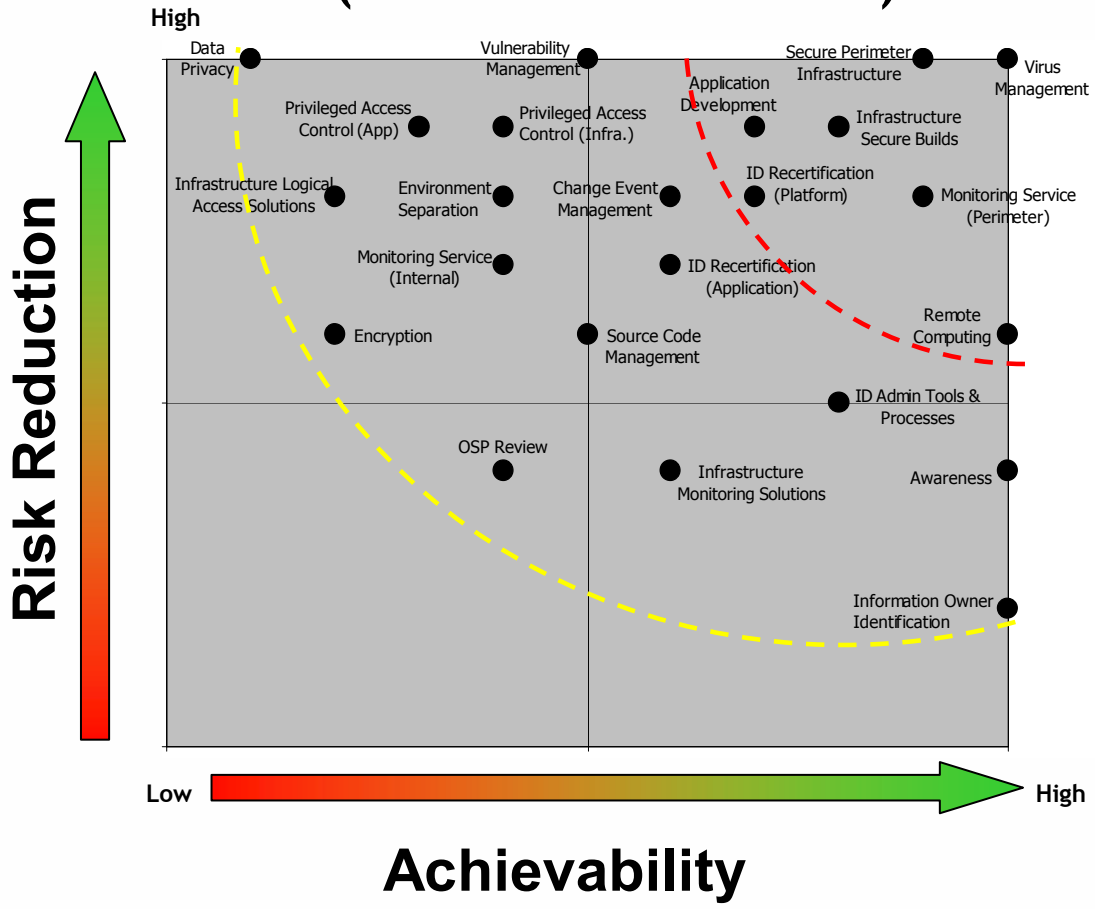
- **Practice zero-based budgeting**
- **Get more efficient with operations**
- **Prioritize risk projects**
- **"Fix the plumbing" – eliminate variance**
- **Leverage a small set of meaningful metrics**

Productivity: Automate and streamline the commodities

- **Apply the same rigor to security operations that we do to general IT Operations**
  - Strong operational metrics and audit trails
  - Standardization and globalization of processes
  - Ruthless focus on efficiency
- **Must take the time to use what we've deployed to enable smart risk-based decisions**
  - Provide data to the people that can action it, and make an informed decision
- **Areas of focus: Identity & Access Mgmt, Security Information Mgmt, Vulnerability Mgmt**

Productivity: Prioritizing Risk Projects

- You can't do everything
- Focus on manageable, bite-size chunks
- Prioritize based on value-added and achievability



Productivity: Fix the Plumbing

"90% of vision is execution, and 90% of execution is communication."
- Ed Miller, President, AXA Financial

- **How many server builds are there in the company?**
- **How many users with local admin rights?**
- **Are those controls really deployed to 100% of the environment?**

Productivity: Leverage Meaningful Metrics

- **Metrics can provide great visibility into core successes, issues, and an organization's risk posture**
- ***"What gets measured, gets done."***
  - W. Edwards Deming
- **But they can also be completely misused and misinterpreted**
- ***"I think the reason many people drift away from baseball is that you have to realize that a great portion of the sport's traditional knowledge is hokum."***
  - Bill James, quoted in *Moneyball*

Productivity: Leverage Meaningful Metrics

- Avoid the perils and pitfalls of metrics
  - Pitfall #1: Measuring the wrong thing
  - Pitfall #2: Not understanding the audience
  - Pitfall #3: Aggregating too much data
  - Pitfall #4: Artificial Accuracy
  - Pitfall #5: Ascribing the wrong message
  - Pitfall #6: Over-report, underdeliver

Areas of Focus for 2008

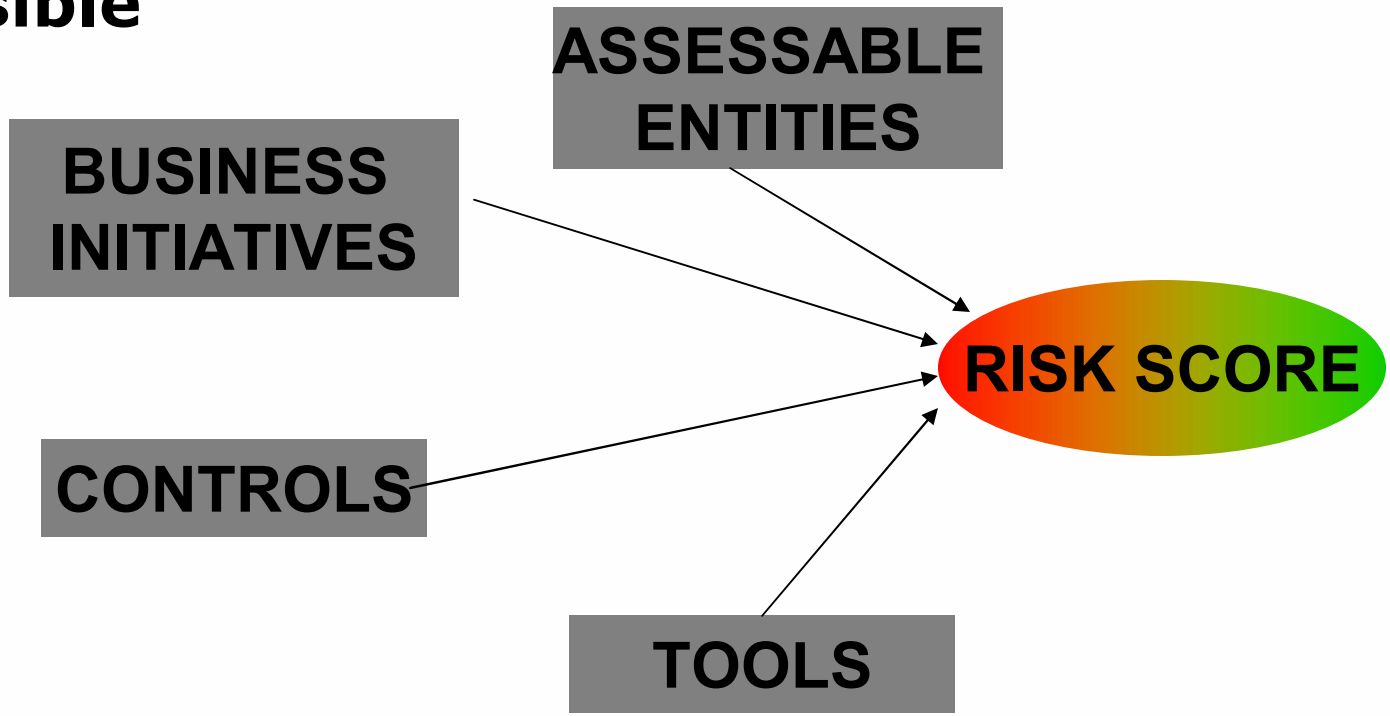
Risk Area	Major Initiative
• Regulatory Scrutiny	• Automated Compliance
• Increasingly Targeted Attacks	• Change in Protection Models
• Privacy & Reputational Risk	• Data Management and Risk Avoidance
• Identity & Access Management	• Automation & Role-based Access
• "Extended Enterprise"	• "Virtual Desktop" and 3rd party assessments
• Evolution of Security into Risk Management	• Linkage with other risk disciplines

#1: Increased Regulatory Scrutiny

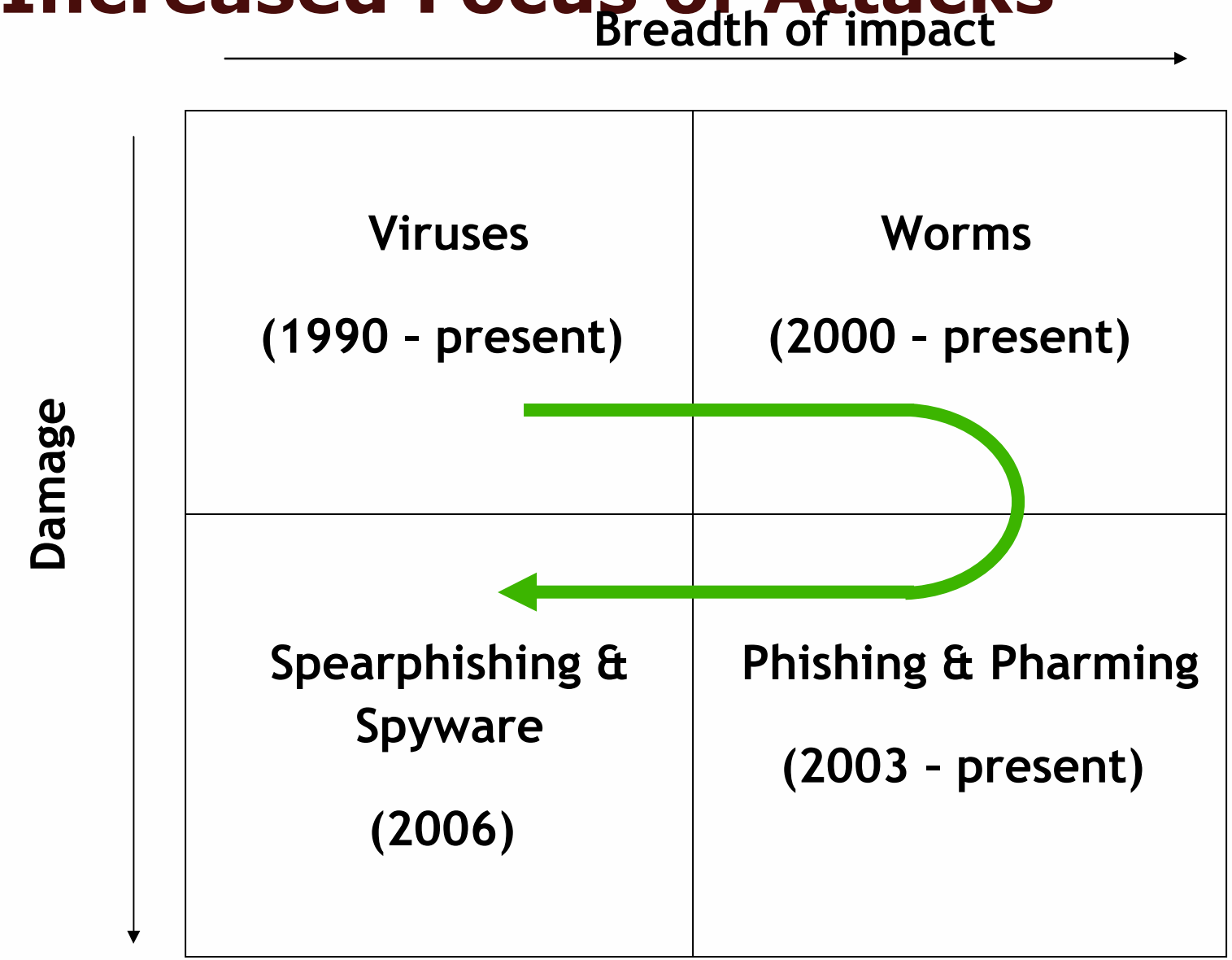
- **The past few years have seen an increase in regulations and compliance requirements**
  - Gramm-Leach-Bliley compliance
  - FFIEC Guidance on Authentication
  - Interagency White Paper
  - Breach notification statutes
  - Sarbanes-Oxley
- **This has required more rigor of existing programs**

#1: Increasing Regulatory Scrutiny

- **Moving from manual assessments to "continuous assessment", automating where possible**



#2: Increased Focus of Attacks



#3: Privacy and Reputational Risk

Data Protection Initiative

- Cover all data, initial focus on PII
- Balance reduction in risk and achievability
- Slow down the *velocity* of leakage of confidential data
- Combination of awareness, technology, and process controls

Areas of Focus

When data leaves the firm

When data is on portable media

When data is widely available

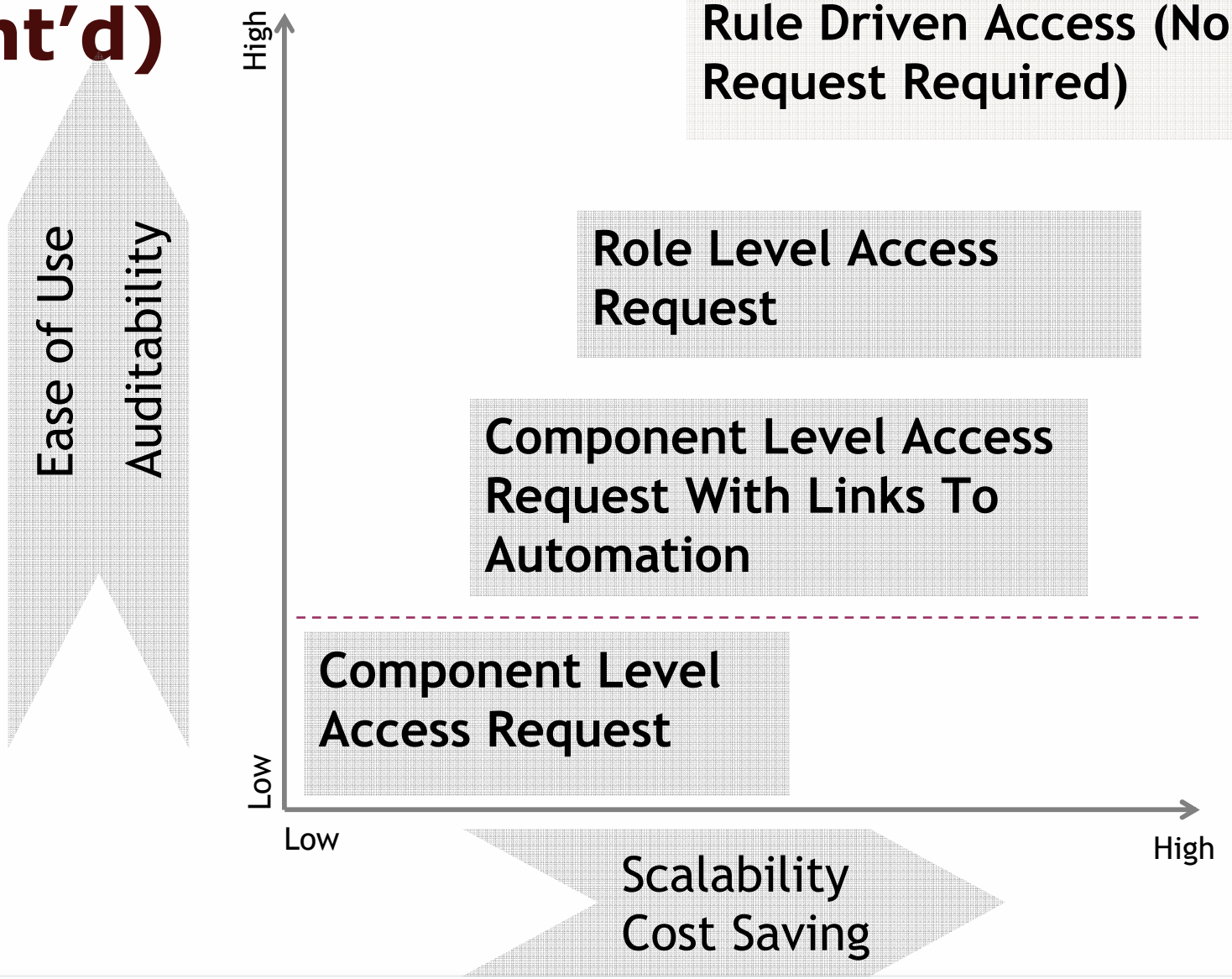
#3: Privacy and Reputational Risk (cont'd)

- **Prioritize efforts based on reducing potential "velocity" of data leakage**
- **Migration to tapeless backup**
  - Core-to-Bunker, Remote-to-Core
- **Controls on portable devices**
  - Laptop encryption
  - Removable media controls
- **Filtering of Personably Identifiable Information (PII)**
  - Email, FTP, HTTP filtering at gateways
  - Discovery of PII on fileshares
- **Application PII remediation**

#4: Identity & Access Management

- **Majority of SOX findings across the industry are in this space**
  - Privileged access
  - Access certification
  - Offboarding / Transfers
- **Significant employee impact**
  - Onboarding
  - General provisioning
  - Complicated and not well-understood
- **Is it an operations group or a security group?**

#4: Identity & Access Management (cont'd)



#5: The Extended Enterprise

- **Companies have become hopelessly "entangled"**
  - "Deperimeterization" of the corporate network
  - The rise of the Outside Service Provider
- **Third-party dependencies abound**
  - Most large organizations have Outside Service Provider (OSP) programs
  - Focused on assessments and contractual clauses
- **Re-evaluate "network-centric" security**
  - Need to migrate to application- and data-centric views

#5: The Extended Enterprise (cont'd)

- **Trend towards alternative desktops**
  - Don't assume a Windows-based PC
  - "Anywhere Access"
- **Increasingly mobile workforce**
  - Access from non-corporate PCs
  - BC/DR support for power users
- **"Ad hoc" connections**
  - Shared suppliers

#6: The Evolution of "Security" Into Risk Management

You want a valve that doesn't leak, and you do everything possible to try to develop one. But the real world provides you with a leaky valve. You have to determine how much leaking you can tolerate."

- Arthur Rudolph, creator of the Saturn V rocket.

#6: The Evolution of "Security" Into Risk Management (cont'd)

- **Need to align with other, more visible firmwide programs**
  - Operational Risk
  - Regulatory Compliance
  - Demand Management and Metrics
  - Partnership with IT Audit
  - LOB presence and execution is a must

#6: The Evolution of "Security" Into Risk Management

- **2004 view:**
  - **We're headed for a schism**
    - Engineering and Operations will move into IT
    - Policy and Strategy will remain separate
  - **Job will split between Risk Management and IT**
    - CISO role will morph into a "deputy risk manager"
    - Focus on maturing the discipline of IT Risk

#6: The Evolution of "Security" Into Risk Management

- **2008 view:**
  - The schism has happened
  - IT security has "grown up" – seat at the table
  - Must apply traditional IT management rigor in order to be given the chance to succeed at executing strategy

"If you don't like change, you'll like irrelevance even less"

- **Tom Peters**