INFORMATION SECURITY | SearchSecurity.com | INFORMATION SECURITY DECISIONS

Justifying Security Expenditures in a Tough Economy: Making the Case for Security

October 21, 2009

Sara Santarelli

Chief Network Security Officer

Verizon

Network Security Services

Verizon Communications

Who We Are

- Premier broadband Internet company in the U.S.
- Leading global communications provider
- Innovative, high-tech leader
  - FiOS Internet and TV
  - Mobile broadband high-speed wireless data
  - V CAST Music and Mobile TV
  - Most connected global IP network for 10 consecutive years
- Serves over 133M customer connections (wireline, wireless, broadband, and TV)

verizon

Source: Telegeography Research 2008

Who We Are

verizon

Verizon Wireless

- Largest wireless company in the U.S. with 87.7M customers
- Most reliable wireless network
- Mobile broadband available to more than 284M Americans

Verizon Telecom

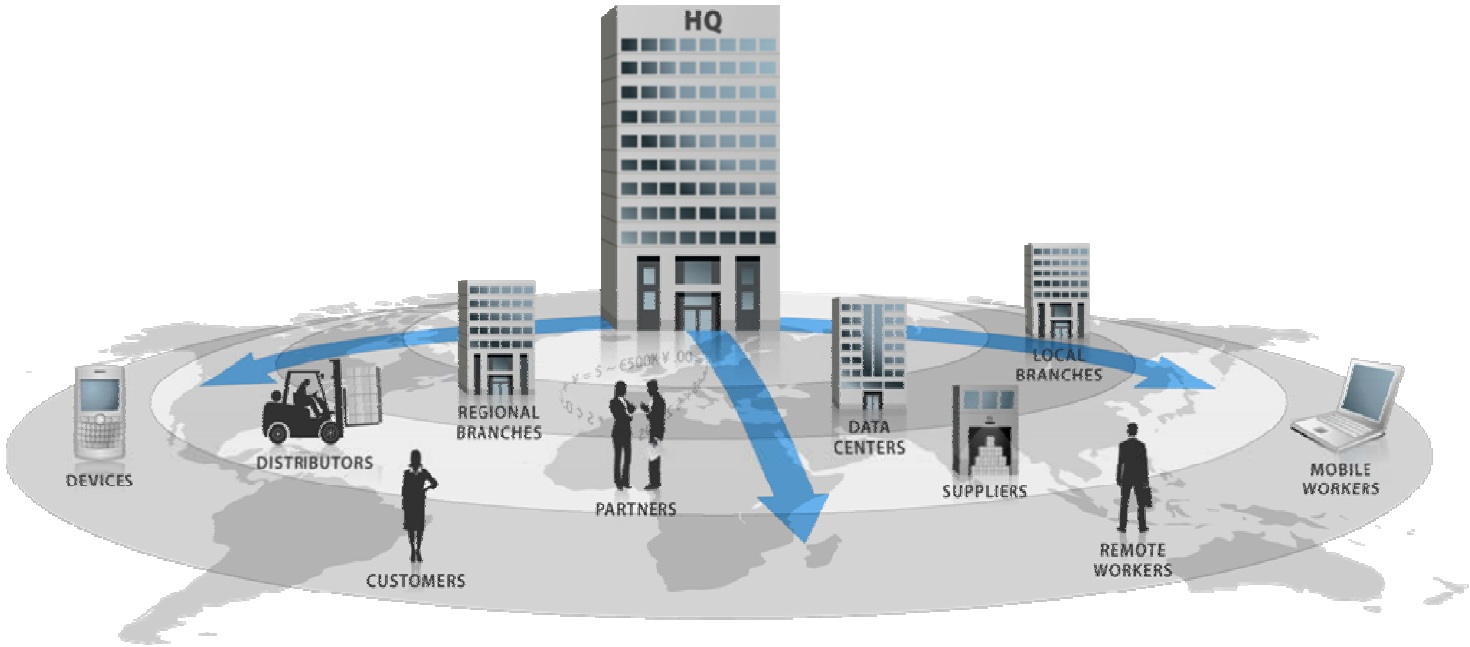
- FiOS Internet: passes 13.8M homes and businesses
- Connects average of 1B telephone calls every day

Who We Are

Verizon Business

- Extended global presence and operations
- Advanced IP applications: VPN, VoIP, and hosting services
- Secure global access to customers in 2,700+ cities and 150+ countries
  - 485,000+ fiber route miles
  - 200+ data centers
- #1 communications provider to the federal government
- 250,000+ customer servers, routers and security devices managed worldwide

The Extended Enterprise



Technology and business have converged to create new challenges

- Business is data, and data is everywhere
- Customers, employees, partners and suppliers are global
- Complex IT, security, communication and networking challenges

- Limited resources, expertise and capital
- Multiple compliance needs and drivers
- Growing environmental pressures
- 24x7 customer service expectations

Business Models Have Changed

Measuring against risk

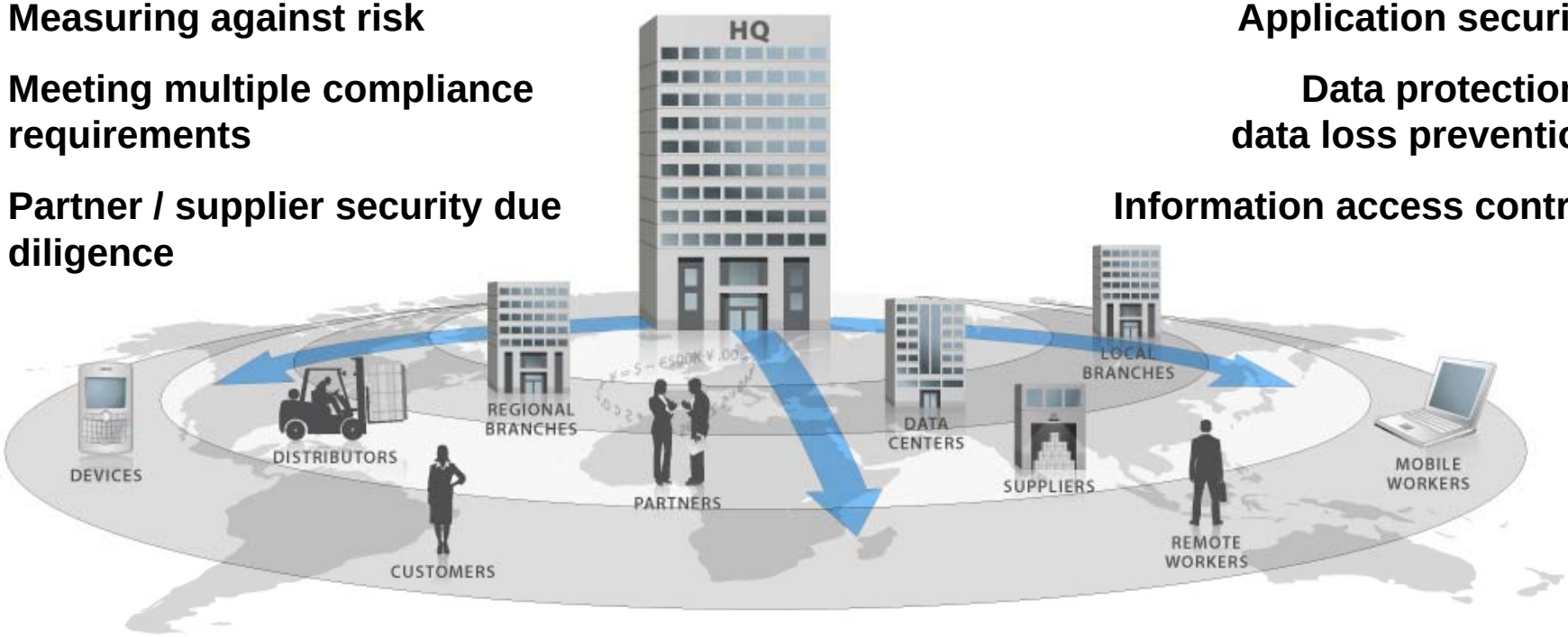
Meeting multiple compliance requirements

Partner / supplier security due diligence

Application security

Data protection / data loss prevention

Information access control



Ongoing monitoring and management

Security log data handling

Business continuity

Consumer / employee mobility

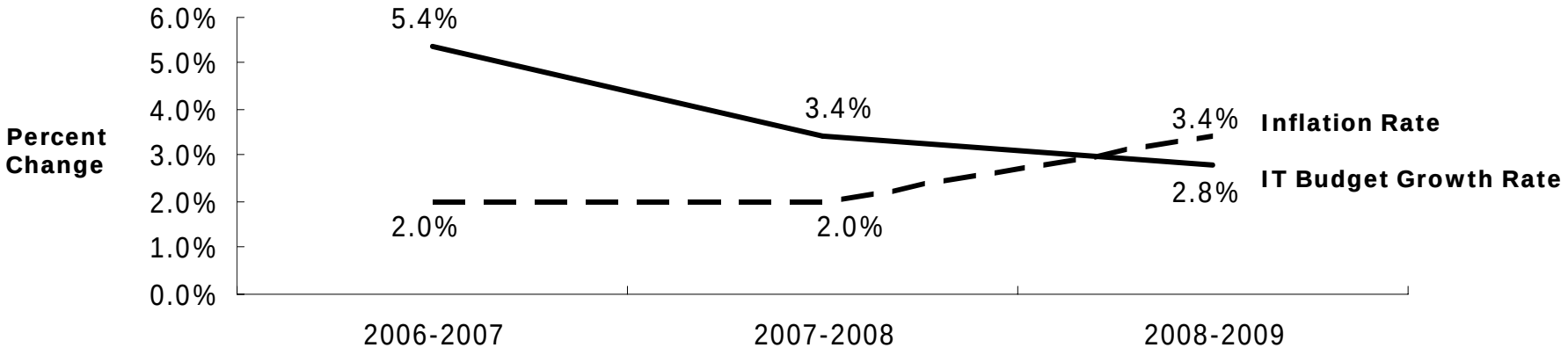
And . . . economic conditions

Economic Climate is Driving Change

- ***Economic Conditions are Driving the Business Model Change***
  - Increased mobility
  - More outsourcing
    - Leads to riskier supply chains
    - Reliance on vendors for QA, testing, and end-user support
  - Capital and technology spending shrinking

Projected IT Budget Growth

2006 - 2009



Source: Corporate Executive Board ©2008

Security is NOT Immune!

CISOs should expect pressures on their budgets and increased risk exposure from third parties

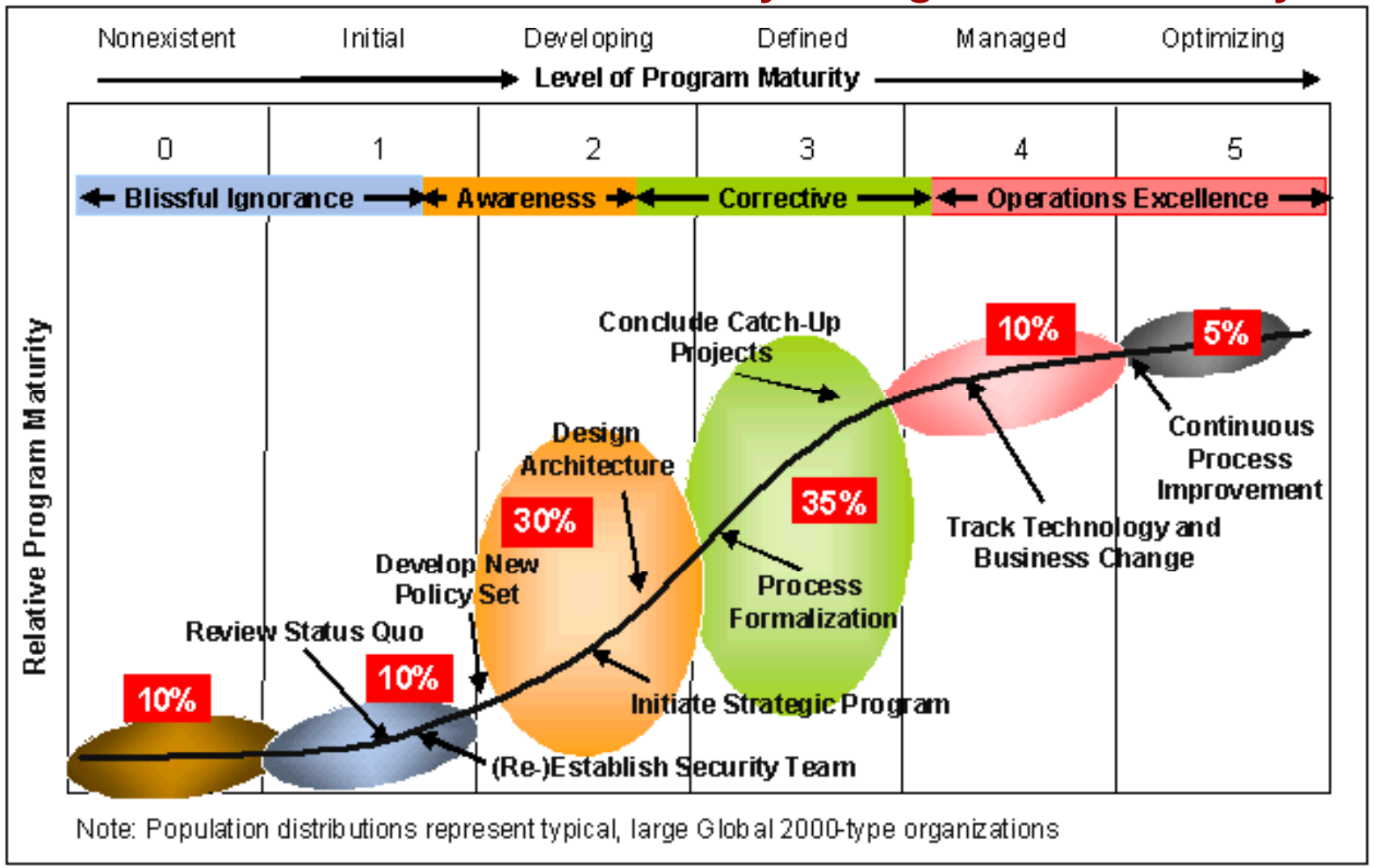
- ***History shows working conditions change as a result of economic conditions to increase the risk of security incidents***
  - Malicious attacks by insiders and recently terminated employees increases
  - Overworked employees take riskier shortcuts
  - Overall "lowering of the guard" is seen across the board
    - Employee effort decreases
    - IT misconduct worsens

Reality check:
Information risk can be dwarfed by other business risks

Source: Information Risk Executive Council

Comprehensive Strategic Approach

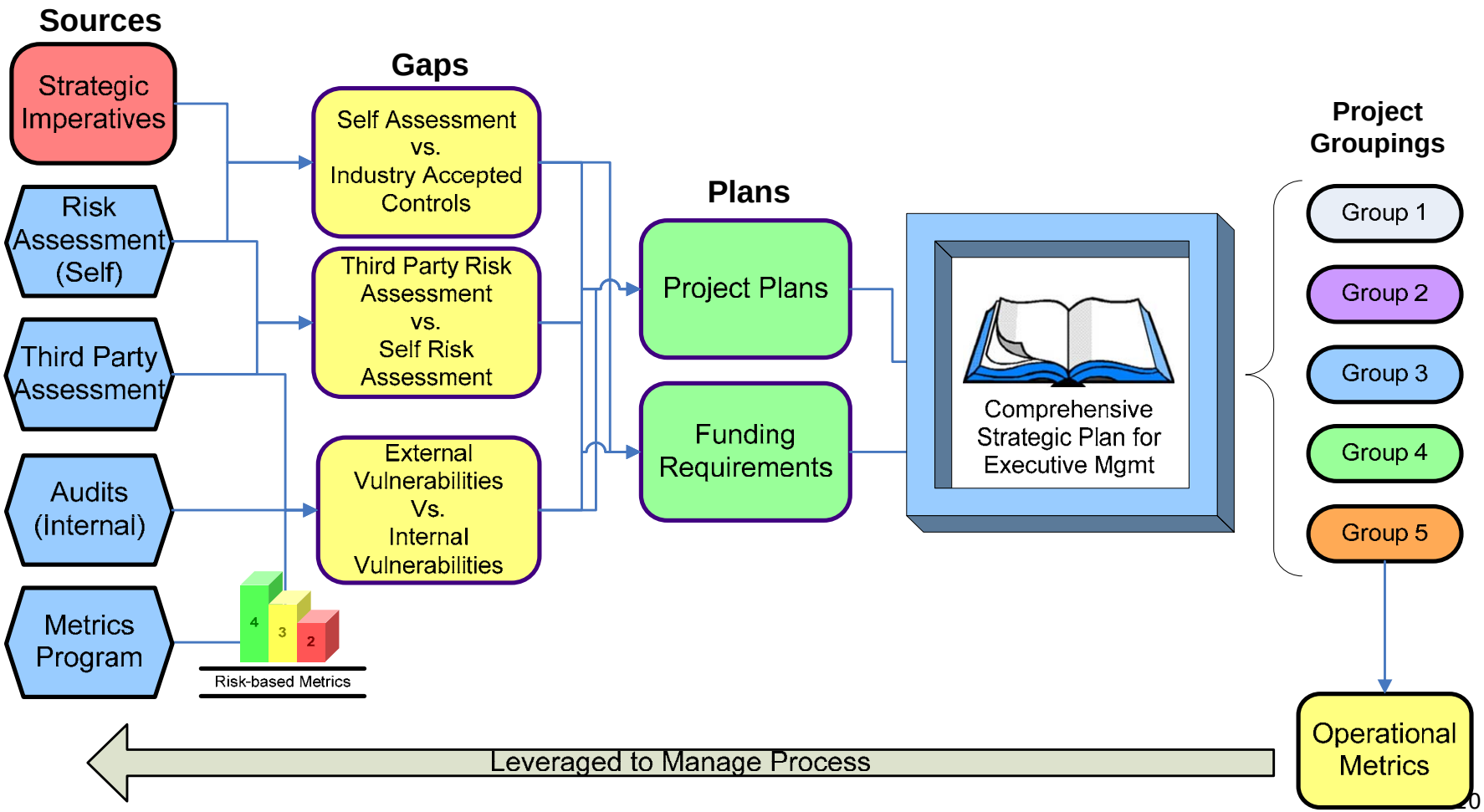
Gartner Information Security Program Maturity Timeline



Gartner -- Best Practices for Moving Up the Information Security Maturity Curve by Tom Scholtz, August 11, 2009

Demonstrating Value

Comprehensive Strategic Security Plan



Comprehensive Strategic Approach

Phase I - Sources

Strategic Imperatives

- ***Align your security plan with your business goals***
- Be willing to adapt to change

  "You can't keep doing the same thing and expect different results."
- Measure and document success

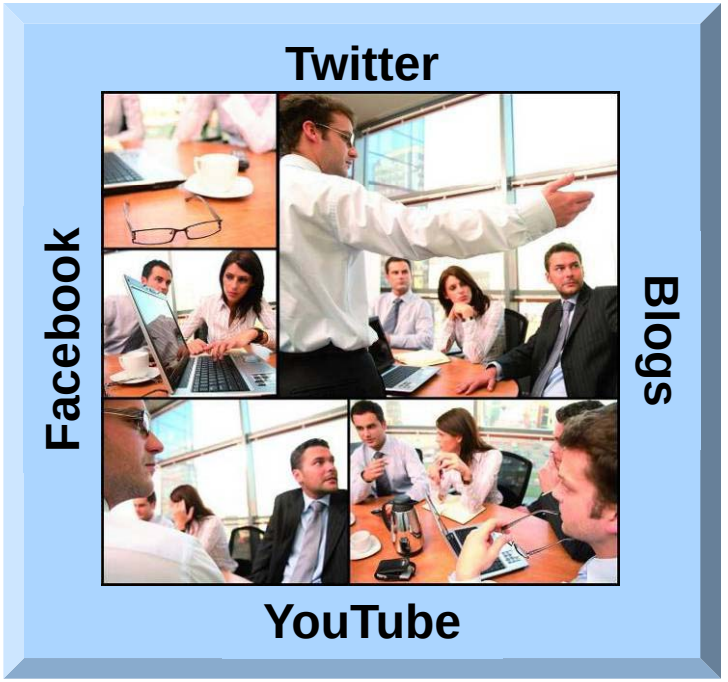
It's not easy to improve process or change business culture

Comprehensive Strategic Approach

Phase I - Sources

Risk Assessment (Self)

- ***Provide a holistic view of security: policies, processes, people, and technology***
- Continual assessment; complete annually
- Include inside SME risk assessment
- Evaluate against industry-accepted controls
- Deliver to executive management
- Utilize as baseline for program maturation assessment year over year

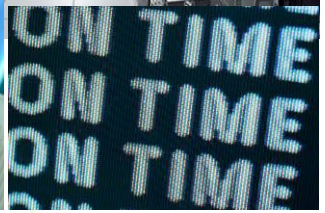


Comprehensive Strategic Approach

Phase I - Sources

Risk Assessment (Third-party)

- ***Provide outsider view of security; identify specific areas for action***
- Include general assessment plus special focus on one or more specific areas
- Formally deliver to executive management
- Utilize as baseline for program maturation assessment year over year



Comprehensive Strategic Approach

Phase I - Sources

Internal Audit

- ***Provide internal view of security; identify specific areas for action***
- Review current internal audit findings
- Identify potential findings from team knowledge and experience

Comprehensive Strategic Approach

Phase I - Sources

Metrics Program

- ***Develop meaningful and measurable risk-based security metrics***
- Review risk-based metrics in place today
- Identify and develop new and meaningful metrics for reporting

Comprehensive Strategic Approach

Phase II – Gap Identification

- Security program gaps create “risk”
  - Risk provides the opportunity for threats to exploit vulnerabilities
    - *Risk = Threat x Vulnerability x Impact (Value)*
- Adjust scope each year to accommodate various factors
  - Economic/business landscape
  - Overarching corporate strategic objectives and imperatives
  - Maturity of the security program

Comprehensive Strategic Approach

Phase II – Gap Identification

Risk Assessment (Self) vs. Industry-Accepted Controls

- ***Compare and contrast: "How well are we doing?"***
- Set a baseline for current performance against industry
- Identify and document gaps

Risk Assessment (Third-party) vs. Risk Assessment (Self)

- ***Compare and contrast: "What did the third-party miss?"***
- Identify and document gaps

Key Point:

Gaps become areas of focus for current plan

Comprehensive Strategic Approach

Phase III – Project Plans and Funding

Detailed Project Plans

- ***Develop strategic remediation plans to close security program gaps identified by risk assessment or internal audit***
- Link to capital and operating plans
- Deliver visibility required for multi-disciplinary project adoption
- Include project details; the more information, the better your plans
  - Include specific projects, objectives, milestones, sources, owners, funding, etc.
  - Identify dependencies (e.g., capital, expense, other organizations, headcount, etc.)
  - Flag projects for easy reference and sorting (e.g., complexity, funding, audit requirement, etc.)
  - Identify target dates

Comprehensive Strategic Approach

Phase III – Project Plans and Funding

Funding Requirements

- ***Identify and document funding requirements***
- Develop funding model; utilize groundwork from phases I – III
  - Easily identify and prioritize projects
  - Develop credibility and justification for funding

Project/Description	Milestones	Q1	Q2	Q3	Q4	Comments
Project 1	Evaluation / Testing / Implementation					Project on track
Project 2	Comprehensive Plan / Executive Briefing					Briefing scheduled for October 21
Project 3	Procure Equipment / Install					Timeframes dependent on vendor
Project 4	Install / Test					Deployment to continue into 2010
Project 5	Installation / Testing / Roll out					Phased implementation
Project 6	Remediation / Re-test					Timeframes dependent on vendor
Project 7	Approvals / Order equip. / Deployment					Installation expected into 2010
Project 8	Develop Comprehensive Plans / Implement					Timeframes dependent on vendor

Comprehensive Strategic Plan

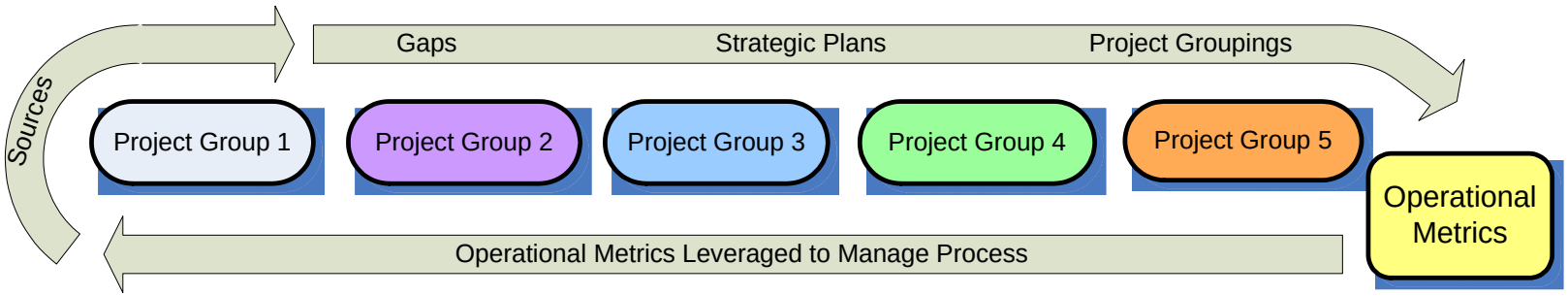
Comprehensive Strategic Plan for Executive Management

- ***Formal strategic security plan***
- Describe plan development approach in detail; phases I - III
  - Comprehensive risk assessment
  - Identification of control gaps
  - Dependencies
  - Complexity, timelines, etc.
- Deliver visibility required for multi-disciplinary project adoption
- Document official request for funding

Comprehensive Strategic Plan

Project Tracking and Operational Metrics

- ***Group projects by imperative and function***
- Update progress monthly
- Provide security program efficiency/effectiveness tracking
- Require a strong asset management program; data security model



Key Point:
Leverage operational metrics to manage process

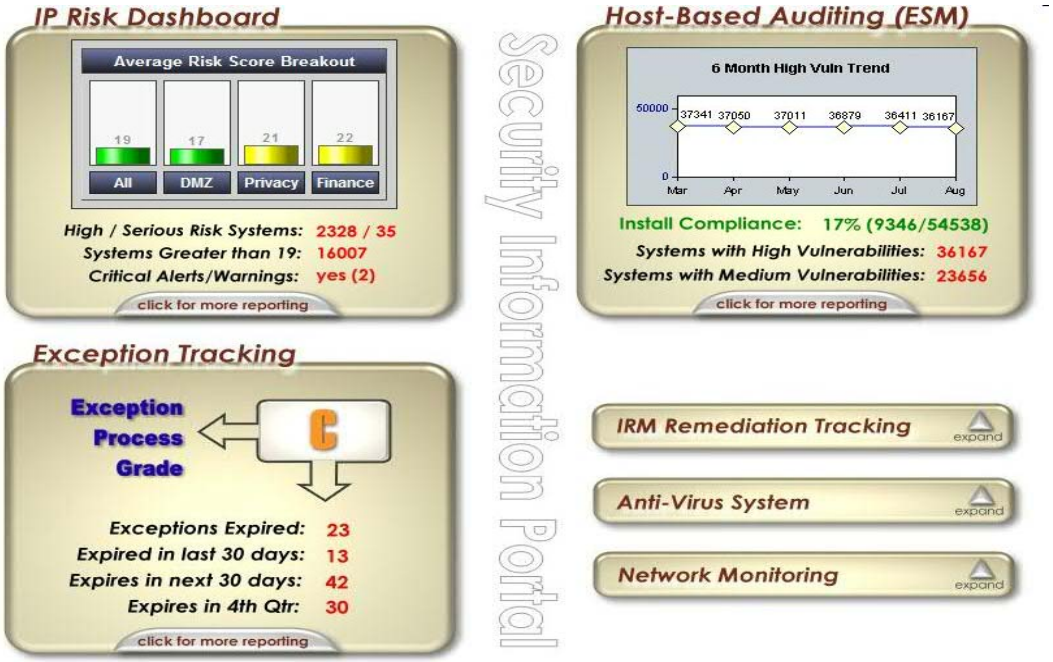
IP Risk Dashboard

Key Technical Inputs

- Vulnerability scan data
- Open ports
- Security standards violations

Risk Score Calculated

- Risk trending over time
- Tracking against asset groupings, based on risk (DMZ, financial, privacy)



Key Benefits

- Owners prioritize list of boxes to remediate
- Executive dashboard to gauge risk levels at a glance
- Security performance reported in relation to peers, company, & subordinates
- At-a-glance view of five worst systems
- Detailed remediation instructions

Where Do You Start?

- ***Sources***
  - Strategic imperatives
  - Review processes and procedures
  - Risk assessment (self)
- ***Gaps***
- ***Plans***
- ***Projects***
- ***Metrics***

What have you done to change your security model?

Questions?