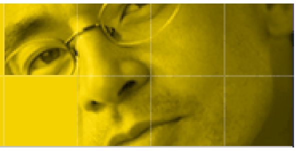
symantec™

Building a World-Class Security Organization

Linda McCarthy

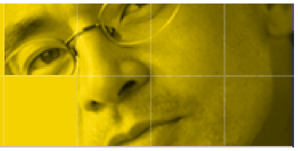
Executive Security Advisor, Office of the CTO

Linda_mccarthy@symantec.com



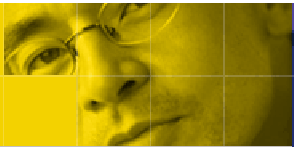
Building a World-Class Security Organization

- Must start at the top
- Do you have a CISO?
- Where does security report in your organization?
- What are your best practices?
- How are your peers doing?
- How do you measure against your peers?
- How do you measure success?



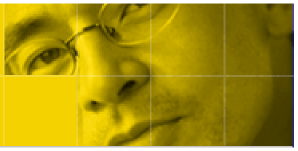
Best Practices

- Different companies – different structures
- Different cultures
- What do you need to protect?
- Healthcare, financial, telecom, technology, and so on
- Funding based on strategic vs. risk
- What are my peers doing in the industry?



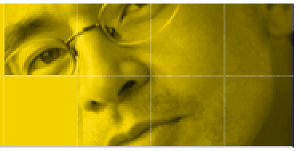
CISO Concerns

- **Pressure to justify security spending:** Increasing scrutiny from management forcing CISOs to demonstrate the business value of security spending
- **Must manage for success:** Need to demonstrate performance excellence to management through better metrics and measurement
- **Working with software organizations:** Managing the complexity of software company relationships from a security perspective
- **Building a world-class organization:** Looking for best practices and examples to follow across different industries

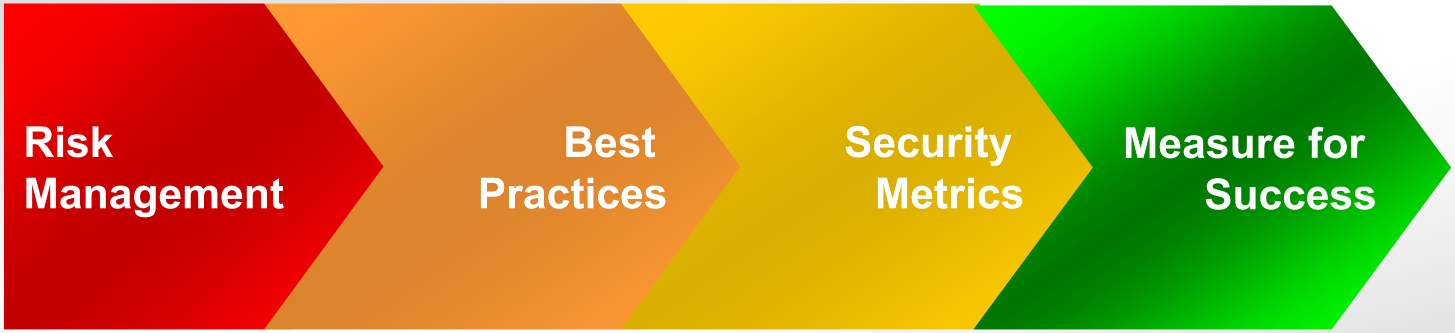


Best Practices in Security

- Changes in managing security - making it pervasive and proactive
- Security management frameworks
- Funding levels and spending prioritization
- Project justification models in use
- Risk assessment models



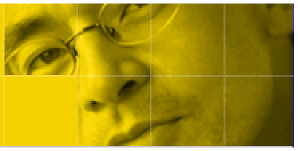
Making Security Pervasive, Proactive and Driven by Results



“Move to Managing Security for Results” Linda McCarthy, Symantec

“Information asset protection is broader than simply protecting intellectual property. We must understand how information flows through the company and to our partners and suppliers to protect the complete eco-system”

On A Comprehensive Approach to Security – CISO High Technology Company



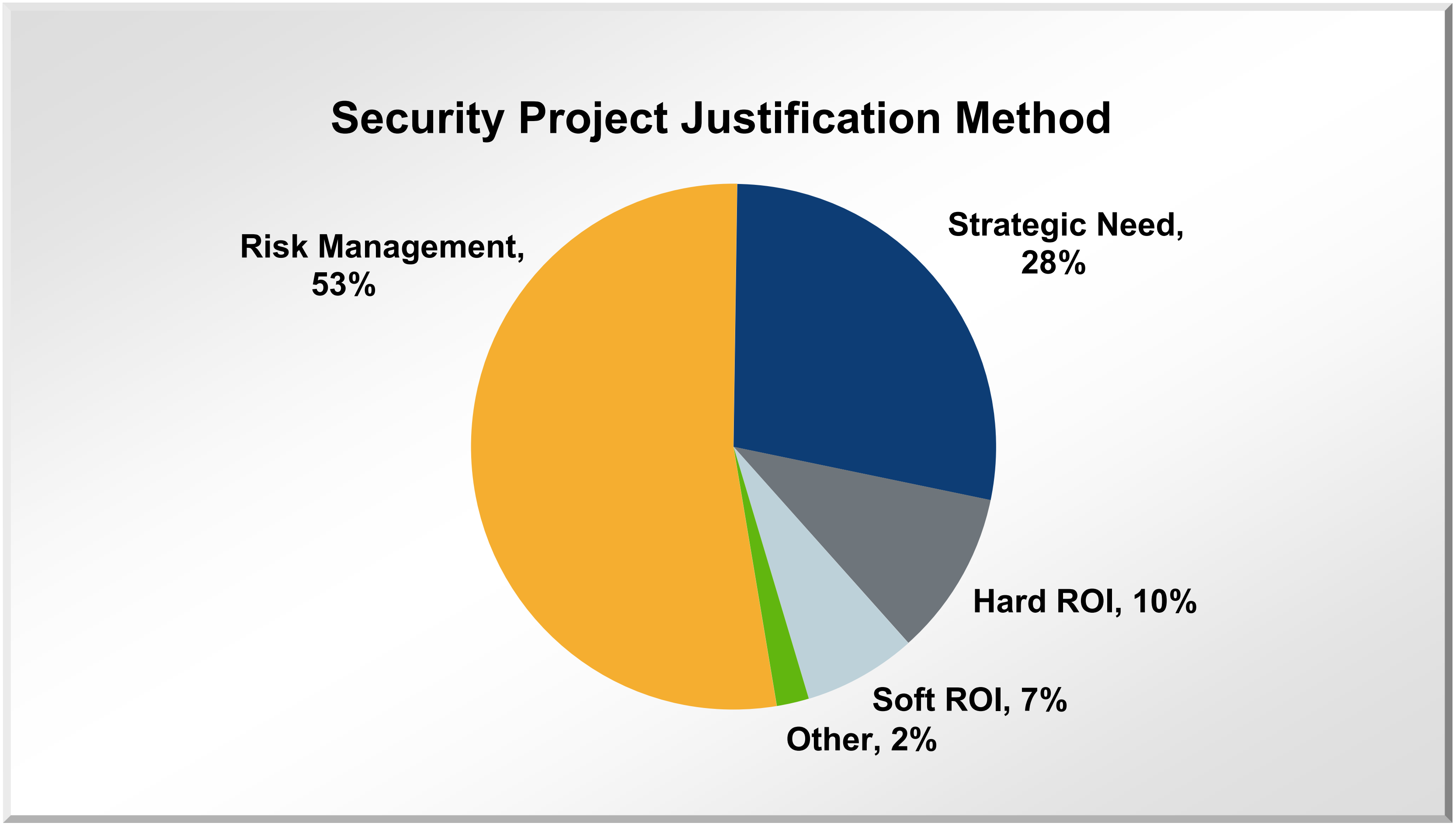
Security Management Frameworks

Areas of control:

- Security Policy
- Organizational Security
- Asset Classification and Control
- Physical and Environmental Security
- Business Continuity Management
- Access Control
- Personnel Security
- Compliance
- Communications and Operations Management
- Systems Development and Maintenance

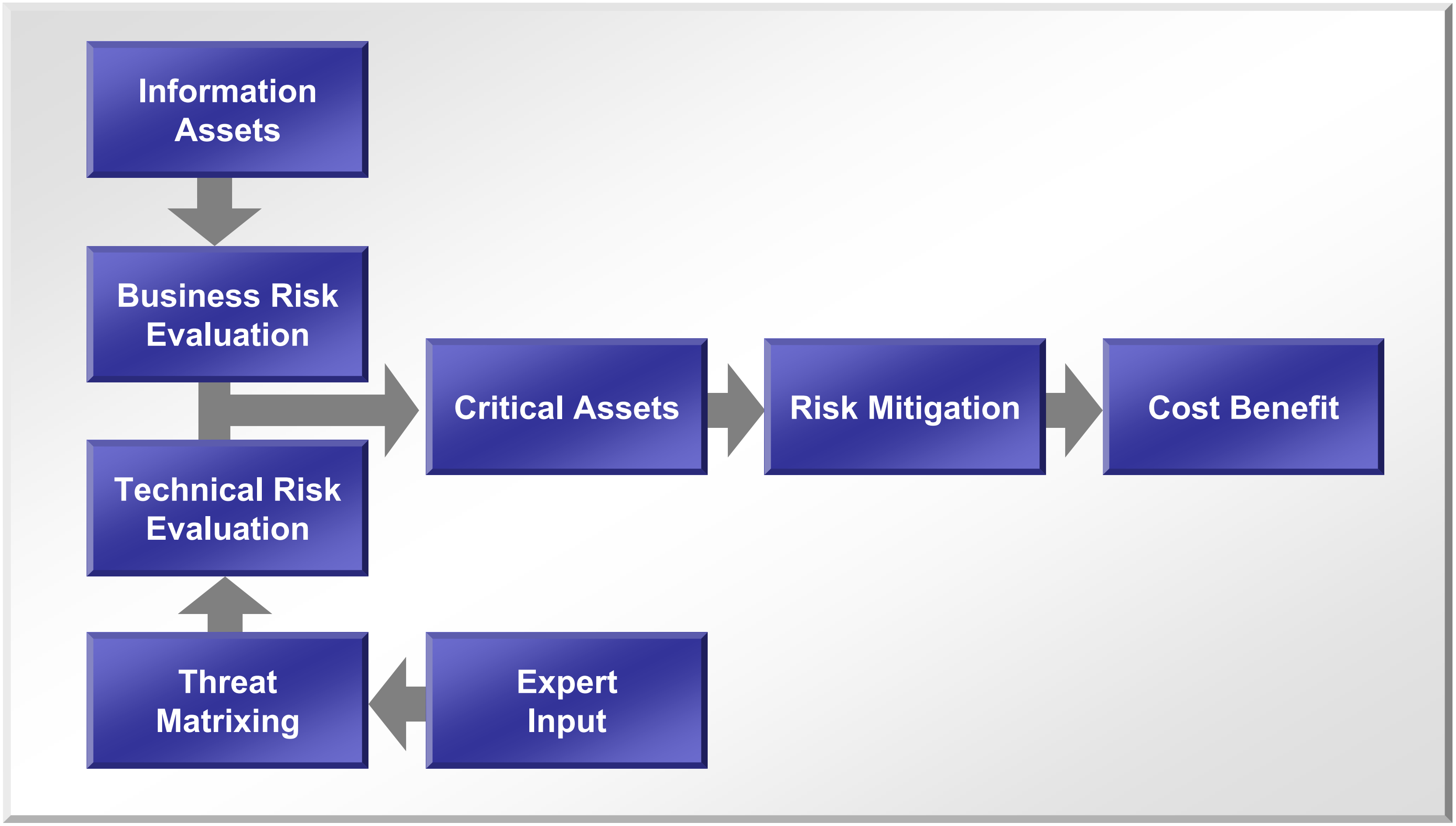
▶ FISMA Reporting Guidelines and NIST resources

Risk Management Reality



Source: Sand Hill Research Report

Understanding Risk Models



Information Assets

Business Risk Evaluation

Technical Risk Evaluation

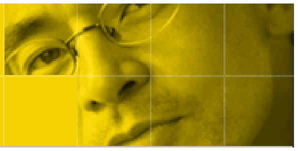
Threat Matrixing

Expert Input

Critical Assets

Risk Mitigation

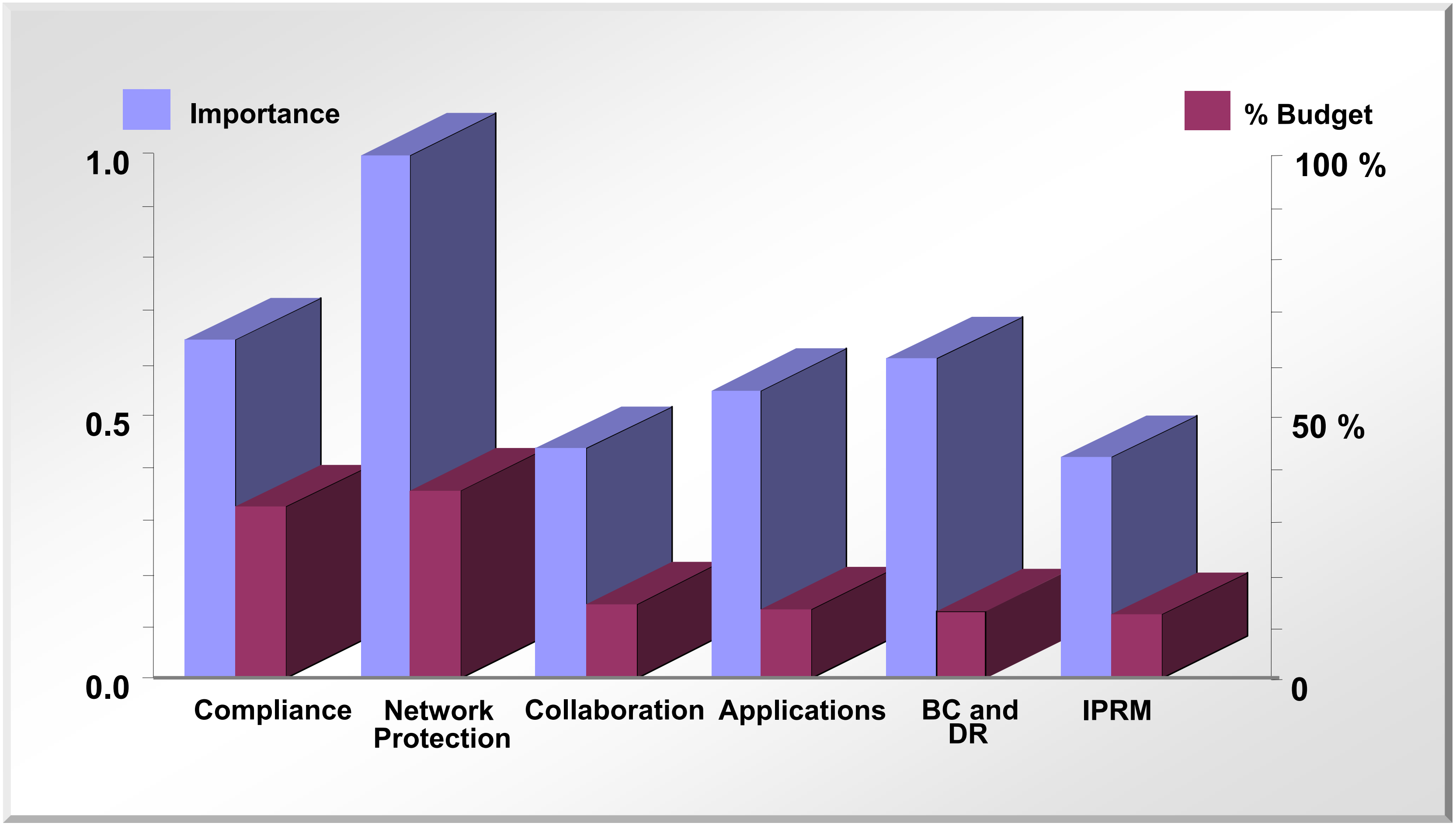
Cost Benefit



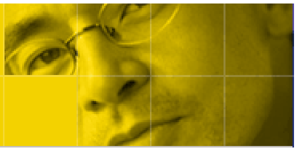
High Priority Initiatives for CISOs

- Next 12-18 months
    - IT Security Policies
    - Security Metrics and Best Practices
    - Application Security
    - Intrusion Detection Management to Prevention Management
    - Outsourcing Partner

Funding Levels and Spending Prioritization



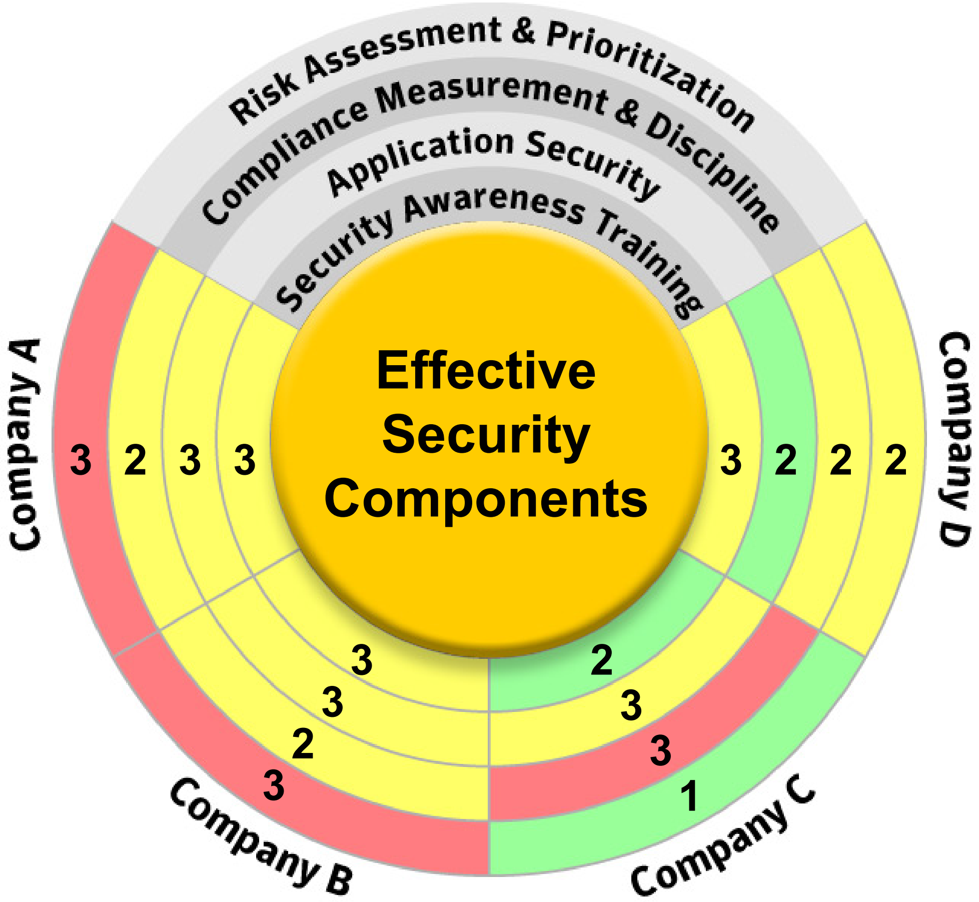
Source: Sand Hill Research Report

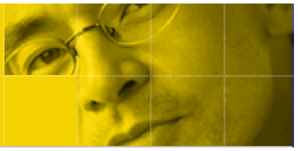


How Do You Measure Up Against Your Peers

- Know what you are doing well
- Know what you need to improve
- Helps increase funding and improve security

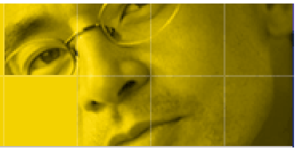
IT Security
Measuring Effectiveness


Risk Assessment & Prioritization
Compliance Measurement & Discipline
Application Security
Security Awareness Training
Effective Security Components
Company A
3 2 3 3
Company D
3 2 2 2
Company B
3 3 2 3
Company C
2 3 3 1



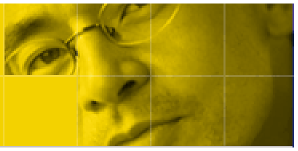
Best Practices – A Top 10 List

1. **Select an IT security framework** such as ISO 17799
2. **Use an IT security risk assessment model** - making sure that the business is engaged
3. **Prioritize IT security projects** with the business
4. **Know how you are doing** compared to your peers
5. **Manage for success, compliance is an on-going process** – you must measure progress continuously

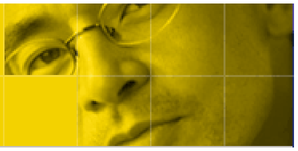


Best Practices – A Top 10 List

6. **Focus spending on important priorities** that you are NOT doing as well
7. **Watch for new laws/regulations as well as business process changes** - your priorities can shift overnight
8. **Use success stories to educate management** and secure funding and support
9. **Look for IT Security "Best Practices" inside as well as outside** your company
10. **Think and act globally -** your Business is global, IT Security is Global as well - know the laws for IT Security and Privacy in all the countries you operate

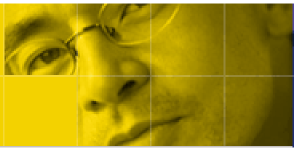


The Need for Security Metrics



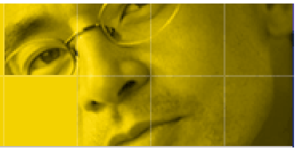
Metrics

- Different companies – different initiatives
- Different security concerns
- Metrics depend on what you are trying to protect and measure
- Where your company stands today
- Have you outsourced everything?
- Are you trying to measure detection and response time?
- Are you still managing operations instead of managing for results?
- Know what your peers are doing in the industry



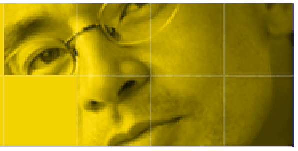
Managing for Success – Need for security metrics

- Security requires a holistic approach – people, process, technology
- Process requires continuity, management frameworks, measurement techniques to determine success
- Performance indicators
  - Describe what we are doing
  - How well are we doing
  - State goals and measure progress
  - Refine measures
- Communicating success – Make sure you communicate success stories to executive management



Establishing Benchmarks – KPI examples

- Risk Assessment
- Vulnerability Testing
- Incident Response
- Infrastructure Protection
- Access Control
- IT Security Training
- Regulatory Compliance

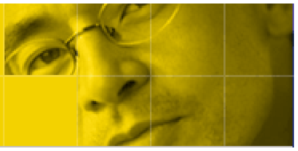


A Security Scorecard

	People			Process			Technology			Customers			Cost		
Functional Domain	P	V	RP	P	V	RP	P	V	RP	P	V	RP	P	V	RP
User Awareness															
Audit Management															
Regulatory Compliance															
Remote Access															
Vulnerability Testing															

P = Performance
V = Value
RP = Relative Performance

Source: Sand Hill Research Report



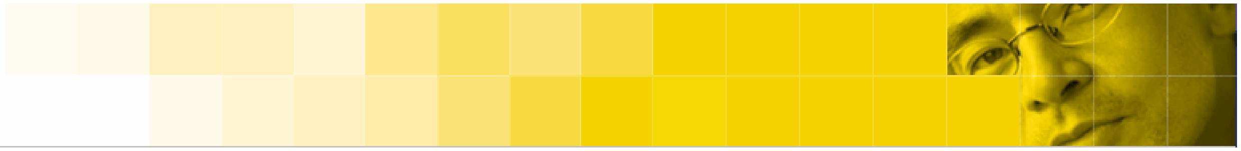
KPI Example

User Awareness Training

- People
  - Performance - % trained/target goal
  - Value – score on tests
  - Relative Performance (RP) – Performance metric / Average
- Process and Technology
- Customers (end users) – similar metrics to People
- Cost
  - Project cost
  - Productivity loss in training

Mindset of the CISO

- What is at risk at your company (assets) ?
- Where are your risks (operations / technology)?
- How do you prioritize and manage your risks?
- What needs to be done to reduce the risks, what’s next…?
- How are you doing, how do you know?



Security Metrics

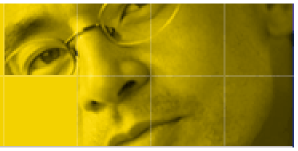
- Build performance, value descriptions tied to your business priorities
- Seek comparisons / benchmarking opportunities in the industry
- Essential for managing risk in multi-sourcing environment and privacy issues

Security Metrics

- Target domains:
    - Infrastructure protection (patches + anti-virus)
    - Virus Management
    - Patch management (time to completion)
    - Vulnerability management (high risk per sys/day)
    - Compliance with Regulations
    - Audit Logs
    - Port Scans
    - Risk Assessment
    - Exceptions granted/not granted
    - Intrusion attempts
    - Policy exceptions

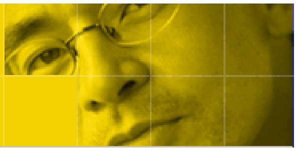
Final Words

- Risk management needs to be a primary focus
- Management may not require ROI, but they must understand the results. Therefore, managing for results is critical
- *Quantifiable* business losses typically from loss of availability
- Measurements need to show positive/negative business impacts
- Need to align risk measurements with your organization’s risk tolerance



Getting Started Metrics – Top Ten List

1. **Understand where you are at risk** (operations/technology)
2. **Prioritize and manage risks** – making sure the business is engaged
3. **Align risk measurements with risk tolerance --** explicit risk acceptance by senior management
4. **Seek comparisons/benchmarking opportunities** – such as IOS 17799
5. **Adapt and improve security processes** – evolving to a more process oriented security organization (such as 6-sigma)



Getting Started Metrics – Top Ten List

6. **Develop metrics and measurements** -- track business goals
7. **Develop KPIs and a specific security scorecard** – change from managing operations to managing results
8. **Know how well you are doing** – compared to your peers
9. **Manage expectations of stakeholders** – senior management – outsourcing partner
10. **Use success stories to educate management** and secure funding and support