



Developing Metrics for Information Security Governance

Interop Las Vegas

April 30, 2008

Presented By:

John P. Pironti, CGEIT, CISA, CISM, CISSP, ISSAP, ISSMP

Chief Information Risk Strategist

Getronics

INTEROP[®]

THE LEADING BUSINESS TECHNOLOGY EVENT

Agenda

- Why Measure
- Key Performance Indicators
- Defining the Measurement
- Metrics Frameworks
- Metrics Libraries
 - Organizational and Professional Metrics
 - Operational Metrics
 - Technological Metrics
 - Business Process Metrics
 - Business Metrics
 - Compliance Metrics
- Reporting
- Final Thoughts

Why Measure?

- Key to Effective Governance
 - Meaningful understanding of business process effectiveness
 - Ability to mature processes for constant improvement
 - Early warning radar for threats and vulnerabilities
- Beneficial Reporting to Management and Business
 - Business aligned knowledge
- Business and Security Intelligence
 - Trend analysis
 - Anomaly detection
 - Threat intelligence



Subjective Vs. Objective Measures

- Subjective Measures
 - Both powerful and harmful
 - High Risk
 - Dependant on knowledge and capability of measuring party
 - Hard to substantiate
 - Human intuition can be the best and worst indicator
- Objective Measures
 - Low risk
 - Supported by data
 - Can be recreated



Key Performance Indicators

- Business Aligned Quantitative and Qualitative Measures
 - Success or failure of processes, personal, technology, organizational effectiveness
- Enable Continuous Improvement
- Facilitate Effective Governance



Defining the Measurement

- What is being measured?
- What is the business value of the measurement?
- Thresholds Should Be Established
 - Positive and negative boundaries
 - Realistic goals
 - Range of values



Gathering The Data

- Electronic Methods
 - System Logs
 - Automated System Monitoring
 - Sensor Networks
- Non-Electronic Methods
 - Statistical Tracking
 - Human Feedback
 - Business Process Monitoring
 - Business Reporting



Know The Audience

- Who is being communicated to?
 - Business audience
 - Technical audience
 - External audience
- Cultural Considerations
 - Localized content
 - Generic language
- Benefits to the business
 - Why does the audience care about the information?



Keep It Simple and Consistent

- Keep it simple
 - Concise and direct measures are most effective
 - Complicated metrics only confuse audience
- Consistency essential for credibility
 - Collect and report in a consistent fashion
 - Provide integrity of information for external reviewers



Business Goal Alignment

- Business leadership and goals define measurement requirements
 - Measures only effective if beneficial to the business
- Map business process to define metrics
 - Visualization can assist in effective metric definition
- Understand motivation
 - How will the metric help the business to be successful?



Baseline Framework of Metrics

- Baseline framework of metrics
 - Foundation of consistent metrics
 - Includes people, processes, procedures, technology and compliance
- Value Provided Vs. Cost
 - Monetary impact
 - Cost of labor
 - Addition of complexity
 - Impact on user experience



Baseline Metrics Framework

Information Security Governance
Baseline Metrics Framework

Business Value

People

Process

Procedures

Technology

Compliance

Information Security Governance Sample Metrics Framework



Common Information Security Metrics

- Number of information security related events
- Number of information security incidents
- Number of media mentions and media types
- Cost of incident investigation and remediation
- Cost of controls
- Elapsed time from incident identification to remediation
- Number of attacks identified
- Number of policy exceptions requested
- Number of policy exceptions granted
- Effectiveness of Controls

Organizational and Performance Metrics

- Measure Organizational Functions Ability to Meet Business Goals
- Measure Effectiveness
 - Provide information infrastructure protection
 - Enable business to run efficiently and efficiently
- Assignment of goals
 - Goals define success or failure metrics



Operational Metrics

- Evaluate effectiveness and capabilities of controls
 - All key controls need to be measurable
- Impact of controls on business activities
- Measure ability of organization to introduce countermeasures and controls
 - How long and how difficult
- Responsiveness to evolving threats and identified vulnerabilities



Technological Metrics

- Provide insight into effectiveness of technological controls
 - Measure capabilities against current attack trends
 - Input from Threat and Vulnerability Analysis used to evaluate measure
- Example
 - Number of spam e-mail messages anti-spam capabilities able to block
 - Number of virus/malware infections detected and prevented



Business Process Metrics

- Impact of information security activities on business activities
 - Security as enabler or disabler to business process
- Utilize business process flow to identify measurable points
- Data points should be represented in dollar values
 - Savings vs. cost
 - Return on investment
- Example:
 - actual material and operational costs for introducing and operating strong authentication capabilities



Business Metrics

- Represent direct impact of information security on business
 - Shareholder Value
 - Market Perception
 - Profit and Loss
- Interaction with leadership team essential for metric development
 - What is important to them?
- Example:
 - Number of negative public media items associated with security incidents



Compliance Metrics

- Measurement of controls required by policy or regulation
- Identification of information required to prove compliance
 - External and internal review
- Trending to prove improvements internal and external auditors
- Example
 - Time elapsed for removal of credentials after termination



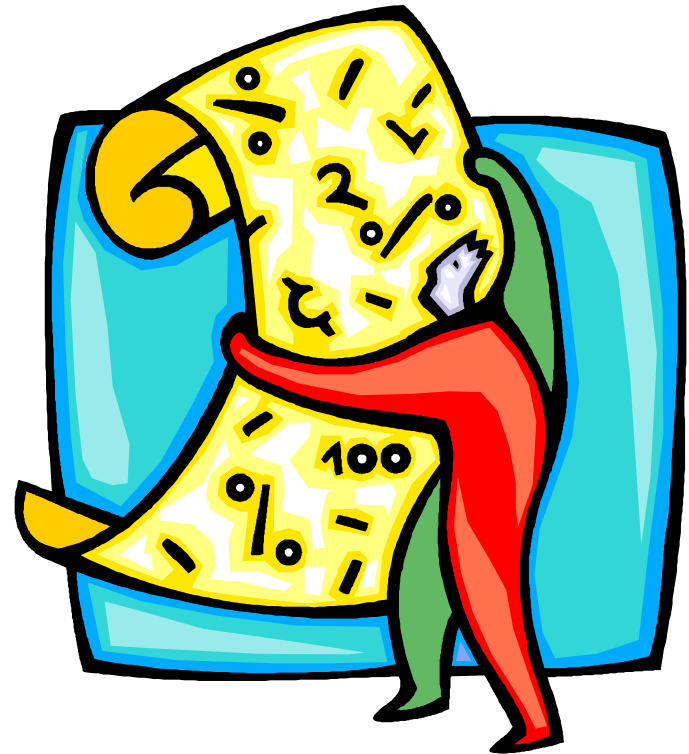
Meaningful Reporting

- Reporting of metrics are important as metrics themselves
- Tiered reporting for different audience types
 - Top Tier: Senior Leadership
 - Middle Tier: Business Process Owners and Managers
 - Lower Tier: Operations and Stakeholders
- Trend Analysis
 - Metrics over time periods
 - Historical values and cycles
- Security Knowledge Management
 - Central repository of data
 - Customized reporting



Reporting Formats and Techniques

- Visual Cues Most Effective
 - Pictures and colors are widely accepted and understood across cultures
 - Human eye most sensitive to color green
 - Red represents danger or attention required
- Number oriented reports useful for quantitative analysis systems
 - Event Correlation Tools
 - Risk Management Tools



Top Tier: Senior Leadership

- Risk oriented information and business impact statements
- Costs and benefits associated with information security
- Market perceptions and customer impacts
- Regulatory Impacts
 - Can they go to jail?



Middle Tier: Business Process Owners

- Effectiveness of controls
- Impact of controls on business process capabilities and efficiency
- Threats and Vulnerabilities
- Regulatory and Compliance Requirement Achievement
- Policy exceptions and audit findings



Lower Tier: Operational Metrics

- Operational status of controls
 - Are they working as designed?
- Functional Boundaries
 - Acceptable limits for controls
 - Tolerance for failure
- Maturity of controls
 - Should they be improved?
 - How can they be better?
 - Do they still make sense?



Frequency of Reports

- Top Tier - Senior Leadership
 - Quarterly
 - Annually
 - Aggregation of Quarterly Data
- Middle Tier – Business Process Owners
 - Monthly
- Lower Tier – Operational
 - Daily or as activities occur

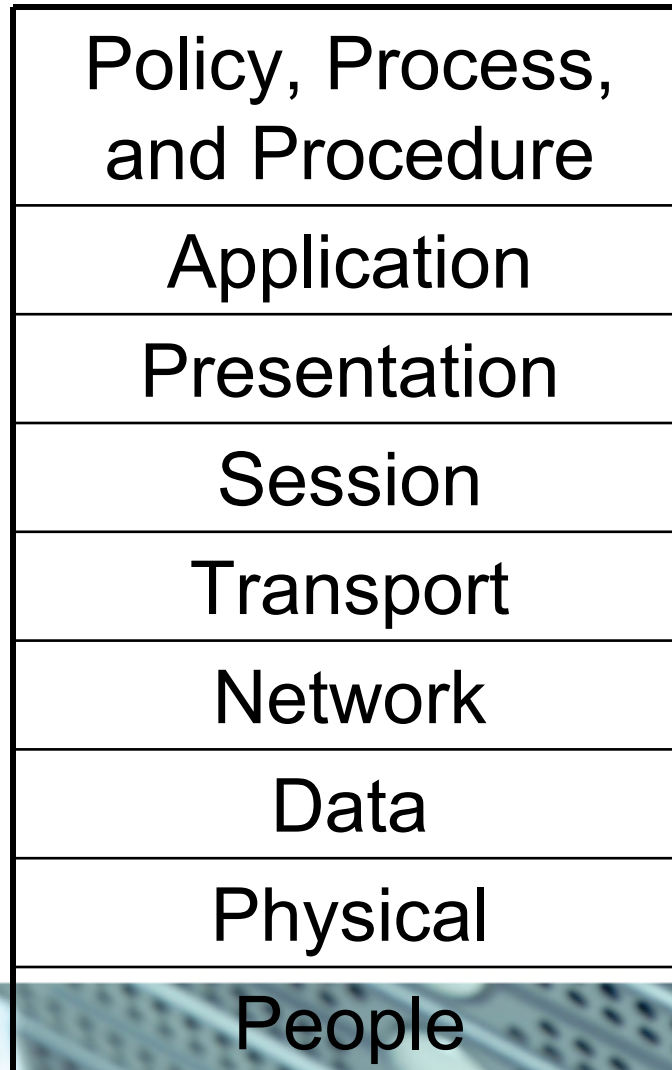


Trend Analysis

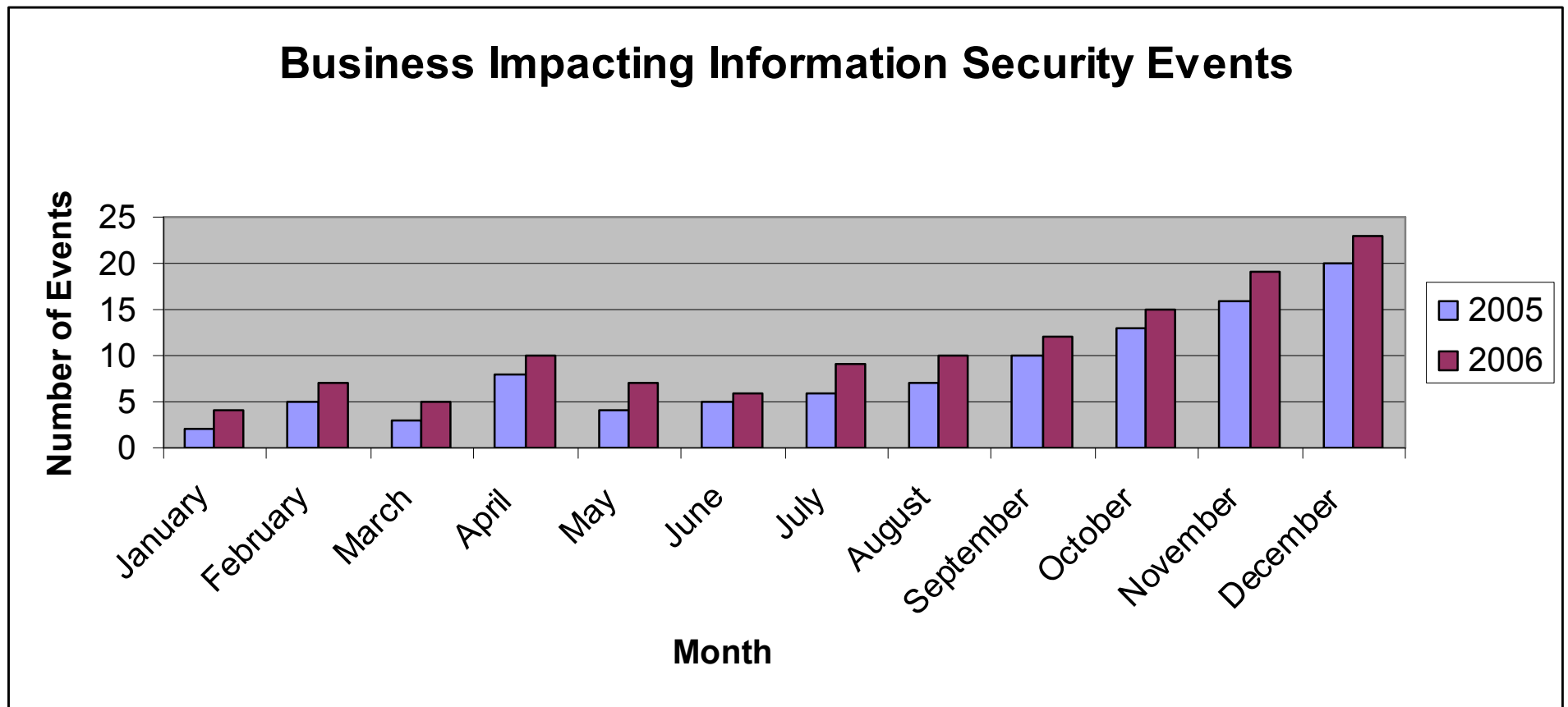
- Mapping metrics over periods of time essential to success
 - History is bound to repeat itself
 - Early warning radar
- Establish boundaries and goals for success and failure
 - Positive and negative business impacts
 - Ensure appropriate level of effort is being applied
- Identification of trends
 - Intelligence for threat and vulnerability management capabilities
 - Identification of new data points for investigation and remediation



Threat Trend Analysis – OSI+ Model



Trend Analysis: Example



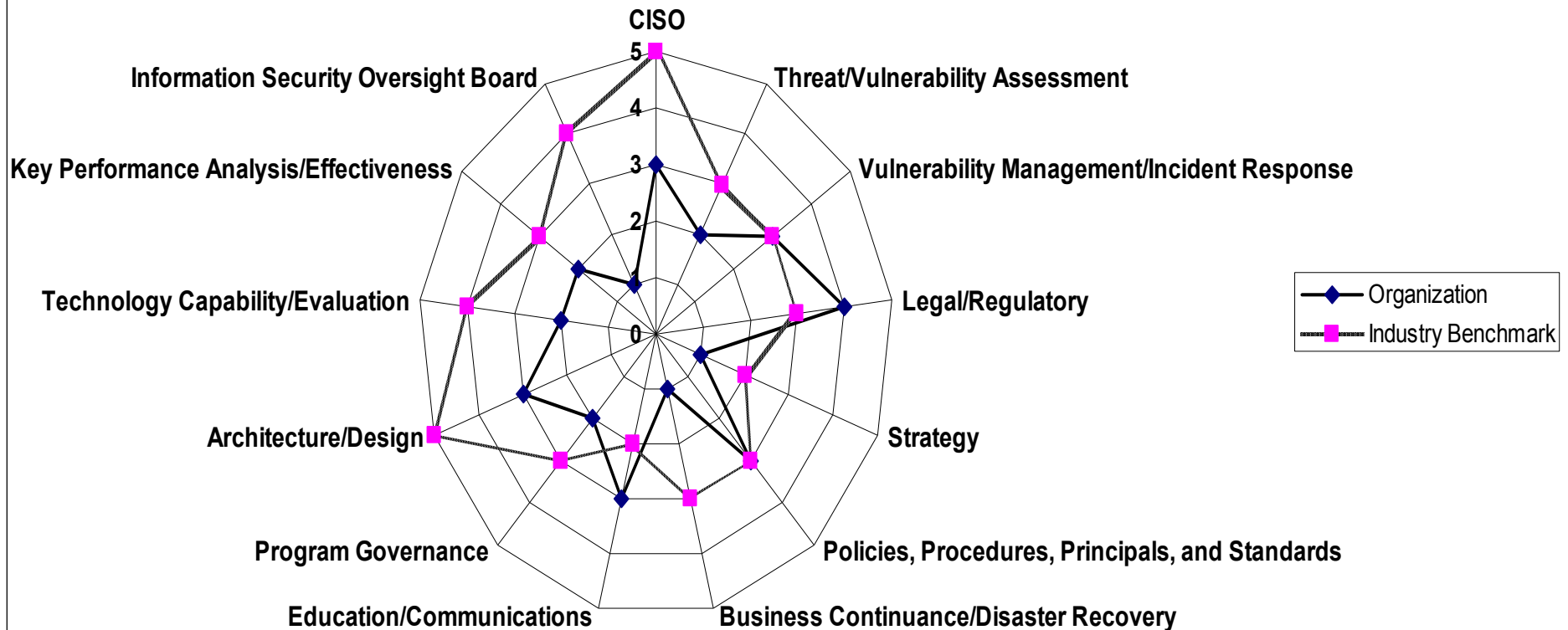
Benchmark Reporting

- Performance of controls and capabilities compared to others
- Industry standards typically easiest to benchmark against
 - CoBit
 - ISO 27001
 - PCI
- Typically survey driven
 - Actual testing provides more accuracy
- Spider maps best way to represent data
 - Immediately recognizable information



Benchmark Report Example

Information Security Program Functional Inventory Capability Maturity Model



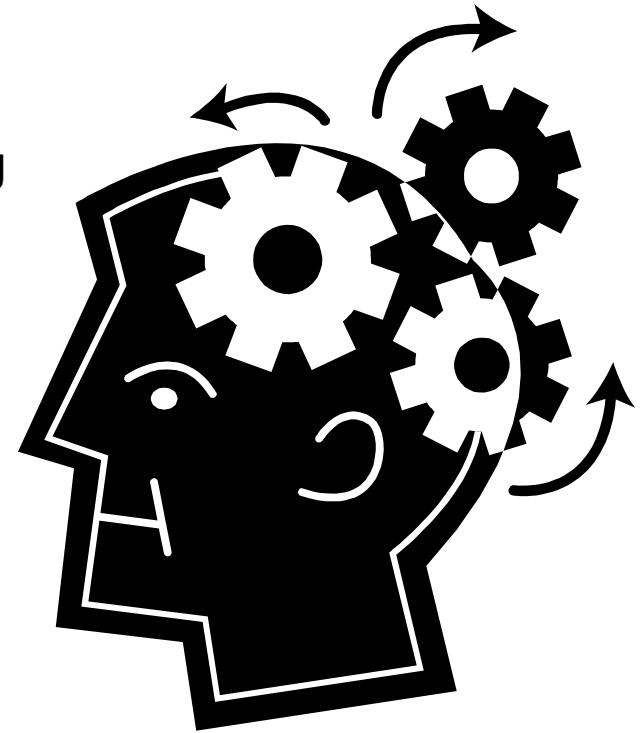
Security Knowledge Management

- Central repository for metric data
- Customized reporting capabilities
- Custom analysis for specific needs and purposes
 - Audit, Compliance, Business Marketing
- Automated report generation and alerting
- Examples include
 - Archer Technologies
 - Control Path
 - RSAM



Final Thoughts

- Information Security is a Moving Target
 - Threats, vulnerabilities, and requirements constantly change
- Effective Metrics Bring Organizational Clarity
 - What threats are realistic and business impacting
 - What vulnerabilities exist in information infrastructure
- Information security Governance Driven By Information
 - Metrics provide knowledge
- Reporting must make sense to the audience
 - Information is useless if it cannot be understood, analyzed, and utilized



Thank You For Your Time!



**John P. Pironti, CGEIT, CISA,
CISM, CISSP, ISSAP, ISSMP
Chief Information Risk Strategist
Getronics
01-978-625-6540
John.pironti@getronics.com**

INTEROP