

Security Performance Management

Dr Paul Dorey
Director, CSO Confidential
Director, Security Faculty



Topics

- Why performance measurement & management?
- What measures?
- Pitfalls & Challenges – futile effort?
- What works for you?

The “hunch to data” model

- Similar experiences
- Several ‘right brain’ data points

Hunch



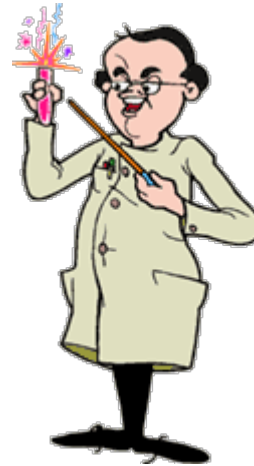
- Outside confirmation
- Logically defensible hypothesis

Expert opinion



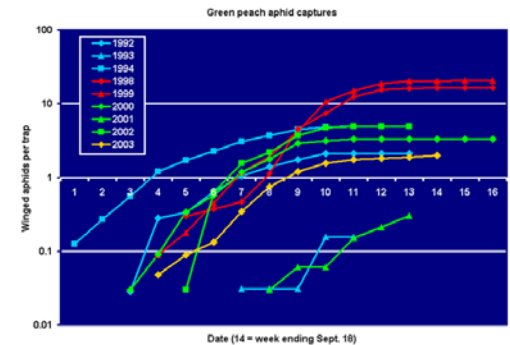
- Data to confirm hypothesis.

Belief evidenced by sampling

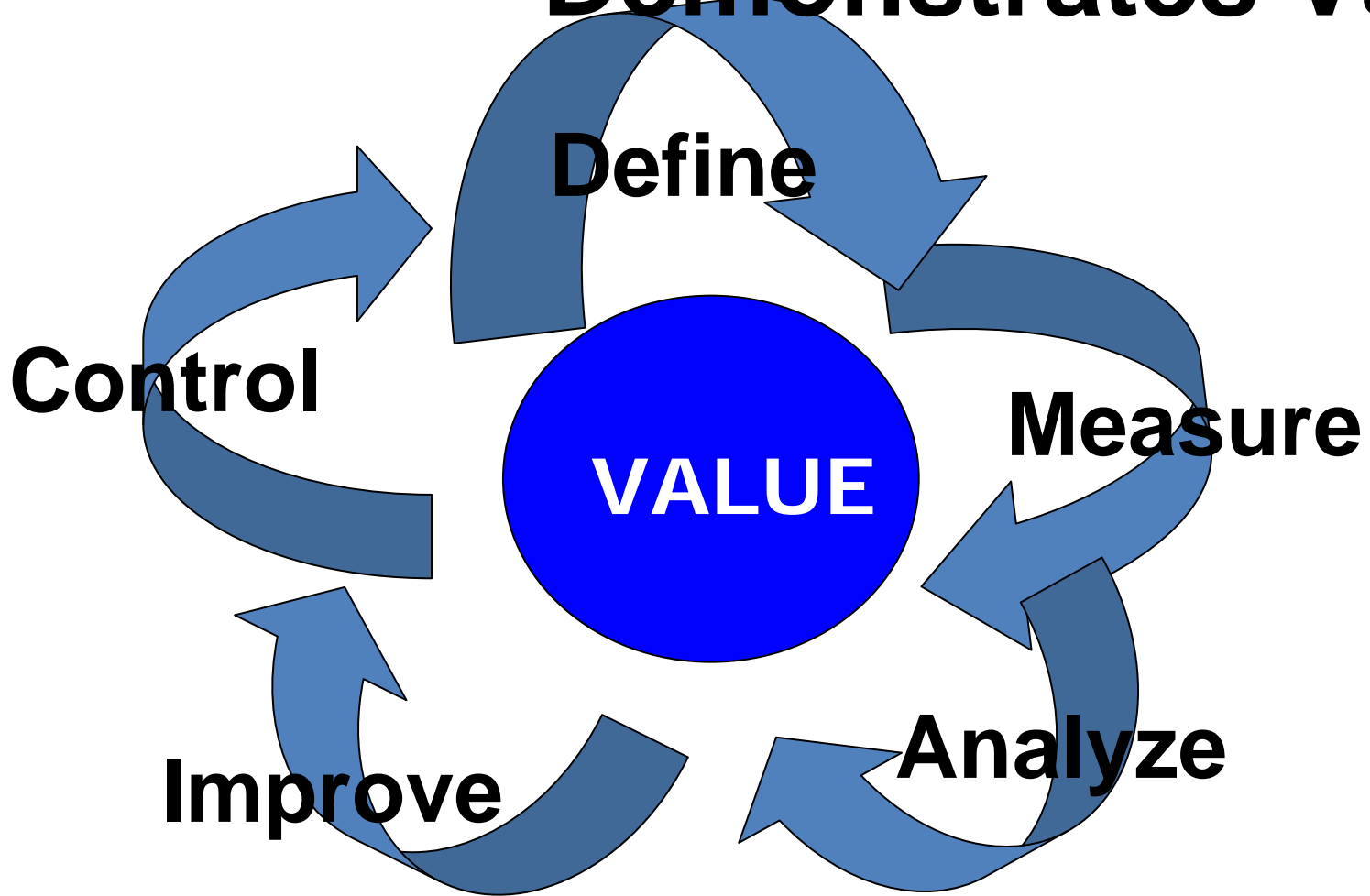


- Large population assessed
- Scale of problem confirmed

Systematic evidence



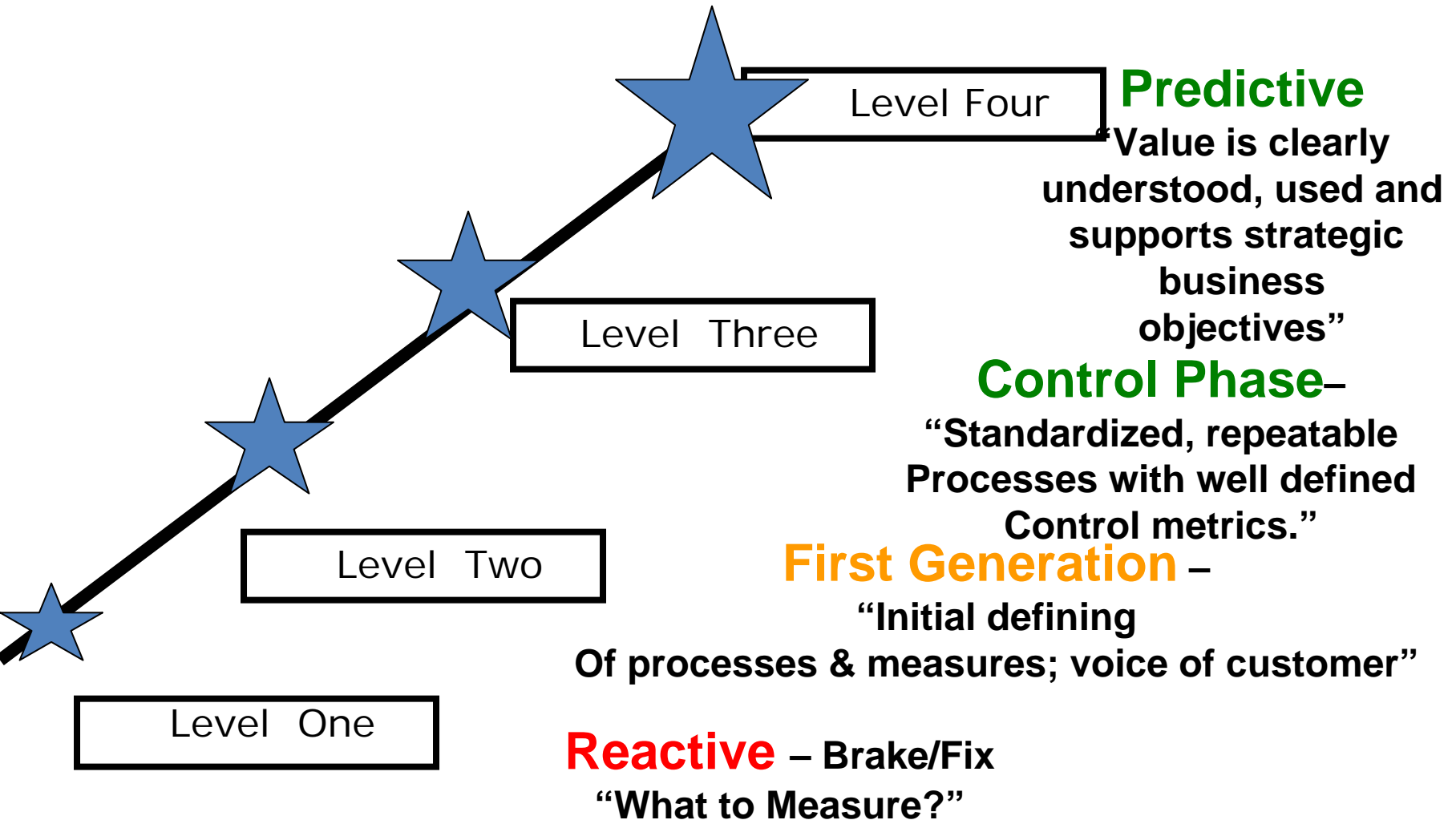
Using Effective Metrics Demonstrates Value



Why Performance management?

- Need to demonstrate value
 - Compliance & Licence to Operate
 - Loss avoidance
 - Business/Cost saving opportunity
- Need to demonstrate prudent use of funding
 - Effectiveness (Doing the right things)
 - Efficiency (Doing them the right way)

Metrics – Maturity Journey



Strategic-measures

Benchmarking:

- Headcount/budget
- Service/Transaction cost

Capability:

- Staff
- Process
- Architectural
- Organisational



Operational-measures

- Advanced Valuation Approach (AVA)?
- ALE, ROSI?
- NPV, ROI?

No level of sophistication is any use unless believed in & used.

To easy to measure what is available vs. what is useful (viruses discovered)

CSO magazine: **Aligning Security Metrics with Business Drivers**

Security Metric	BUSINESS DRIVERS						
	COST MGMT.	RISK MGMT.	ROI, VALUE	LEGAL REQ.	POLICY REQ.	LIFE SAFETY	INTERNAL INFLUENCE
Percent of continuity plans tested, remedial actions completed	●	●	●		●	●	●
Security cost as percent of total revenue	●		●				
Safety hazards eliminated per year, number of		●	●	●	●	●	●
Critical information assets residing on systems with approved architecture		●			●		●
Business control weaknesses identified after investigations or other feedback		●	●				●
Percent of third-parties with confirmed infosec and business continuity requirements		●			●		●
Percent of security incidents where damage did not go beyond acceptable threshold	●	●	●				●

Actions

- Review current plan & capabilities – stop something & identify new priority work
- Test right balance of people/tools embedding/outsourcing/specialist work
- Duplication with other teams – compliance?
- Test right balance of ‘onshore’/’offshore’
- Review architecture (duplicates?)
- Agree value & performance metrics & report

Questions?

paul.dorey@csconfidential.com

