Metricon 2008

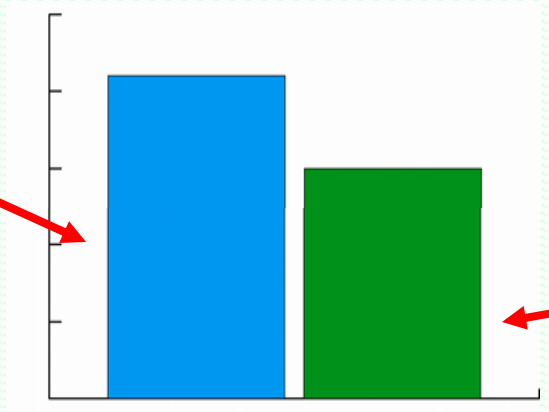
Metrics for Risk Management versus Metrics for Security Attribution

Jennifer L. Bayuk
jennifer@bayuk.com
www.bayuk.com

Compare: Risk vs Security

Measures:	Compliance
Reflects:	Organizational Structure
Favors:	Automation
Demonstrates:	Trends

Compare: Compliance

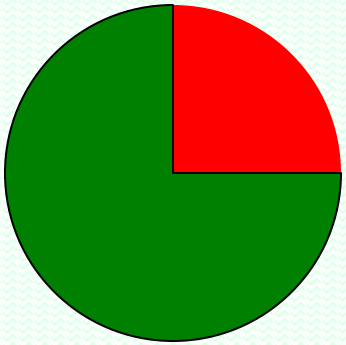


Total Population

Population in compliance

Often based on self-assessment reporting.

Population not in compliance

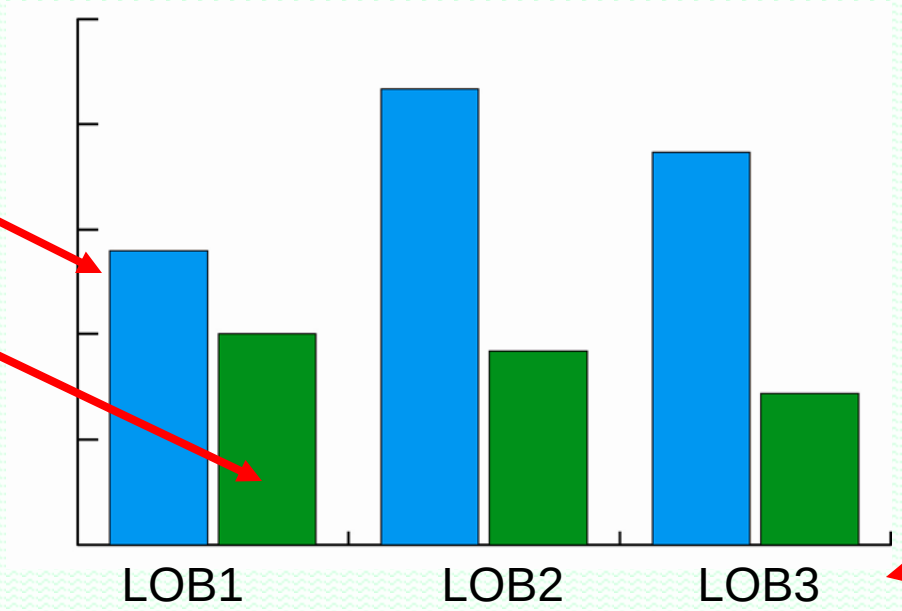


Population in compliance

Compare: Organization

Total Population

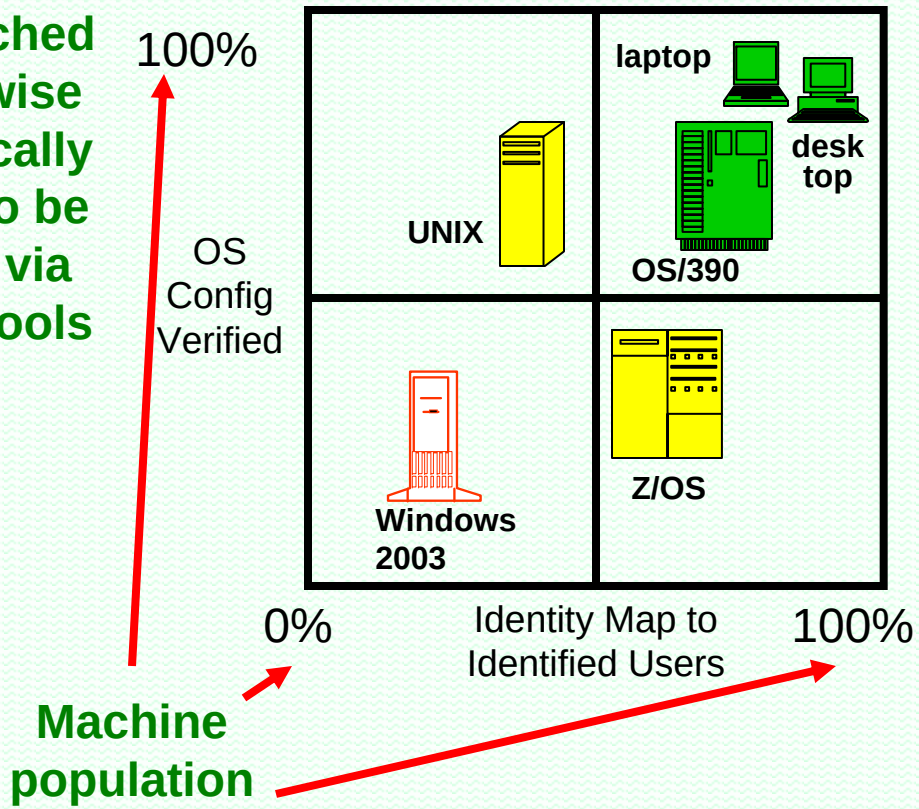
Population in compliance



Facilitates comparison between different sets of management

Compare: Automation

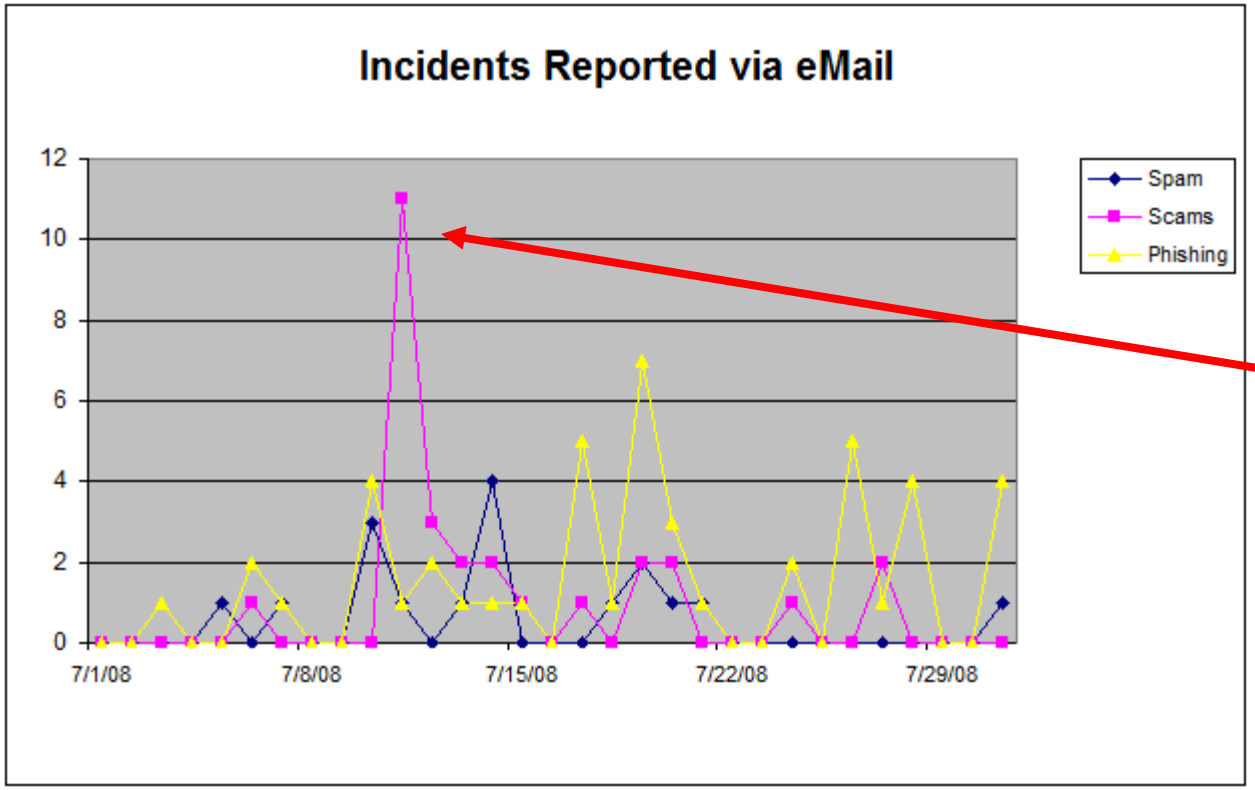
Total patched or otherwise automatically verified to be secured via specific tools



Facilitates comparison between different types of technology, often used for audit remediation.

Compare: Trends

Often used to depict activity beyond control of management



Facilitates demonstration of staff activity requirements

Note: blank lines indicate no incidents were reported, mostly weekends.

Contrast: Risk vs Security

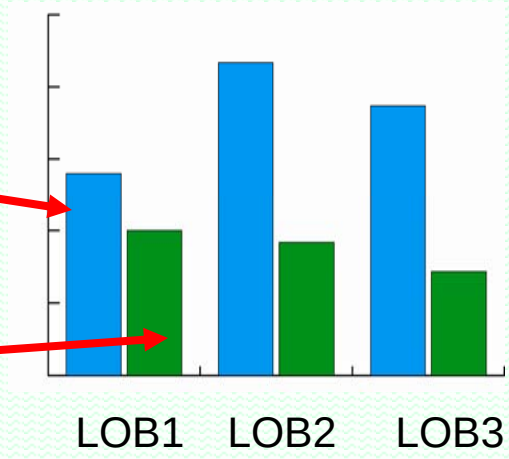
Focus is:	Coverage	Quality
Based On:	Policy	Process
Relies On:	Explanations	Accountability
Reflects:	Assessment	Implementation

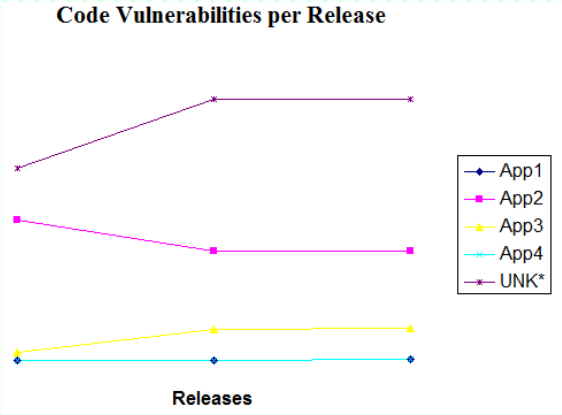
Contrast: Focus

Risk *Coverage* vs Security *Quality*

Total Number of applications

Total applications scanned for code vulnerabilities



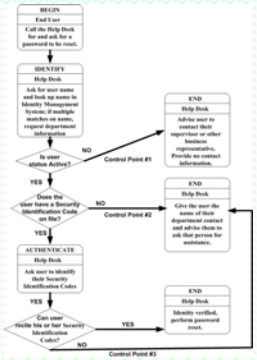


Focus on quality of security results in this type of report

Confidence in totals comes with aggregation rather than collection.

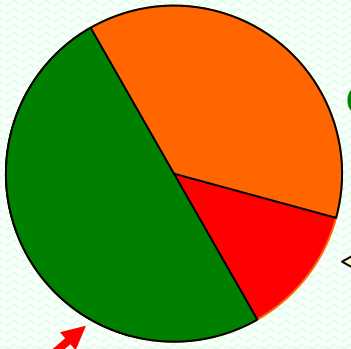
Contrast: Basis

Risk *Policy* *vs* Security *Process*



Population with authorized exceptions to compliance

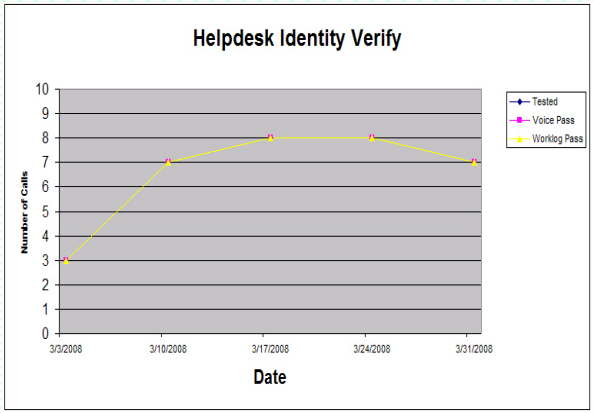
Population not in compliance



Population in compliance

Security managers look for correlation.

Control points from process directly correlated to measured activity.

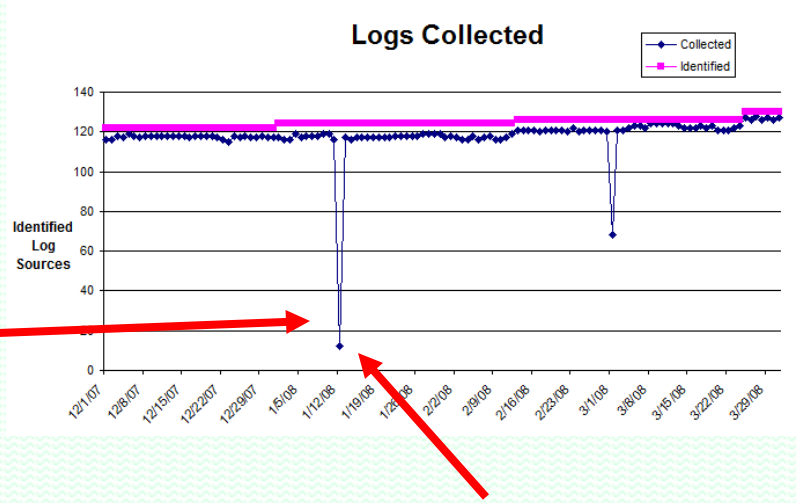


Contrast: Reliance

Risk Security

Explanations vs Accountability

Risk manager hears proximate cause, e.g.: "server down"



Security manager should ask: "What was root cause?"

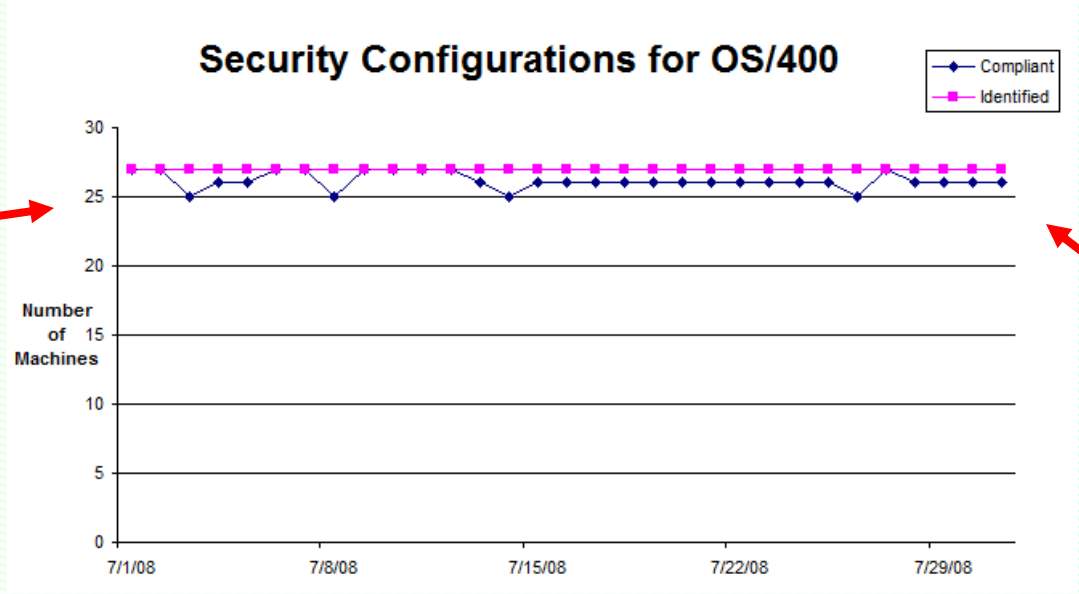
Where there is a process in place designed to maintain the metrics, there should be accountability for poor results.

Contrast: Reflects

Risk Security

Assessment vs Implementation

Risk manager see no dramatic changes



Security manager sees systemic issue

Detail behind OS Comparison from "Automation" example

Prevalent versus Necessary Metrics

What makes security an attribute?
How to find it?
What objectives are met using only risk metrics?
Should overlap be pursued or avoided?

Questions? Discussion…

jennifer@bayuk.com
www.bayuk.com