Metricon 2008

Metrics for Risk Management versus Metrics for Security Attribution

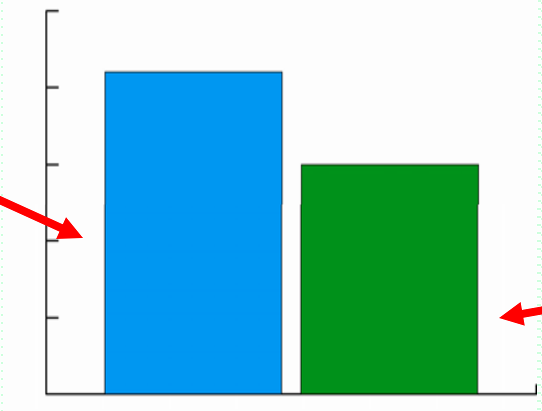
Jennifer L. Bayuk
jennifer@bayuk.com
www.bayuk.com

Compare: Risk vs Security

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

Compare: Compliance

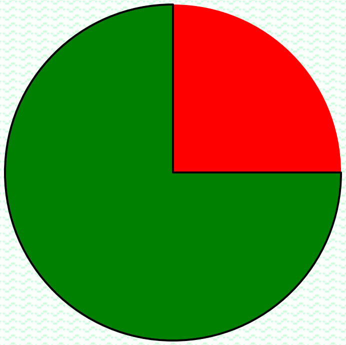
Total Population



Population in compliance

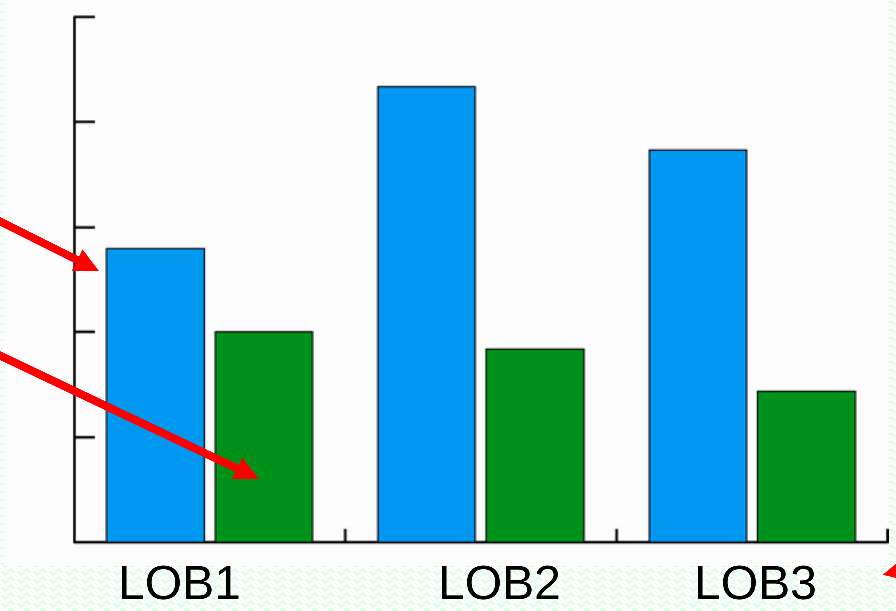
Often based on self-assessment reporting.

Population in compliance



Population not in compliance

Compare: Organization



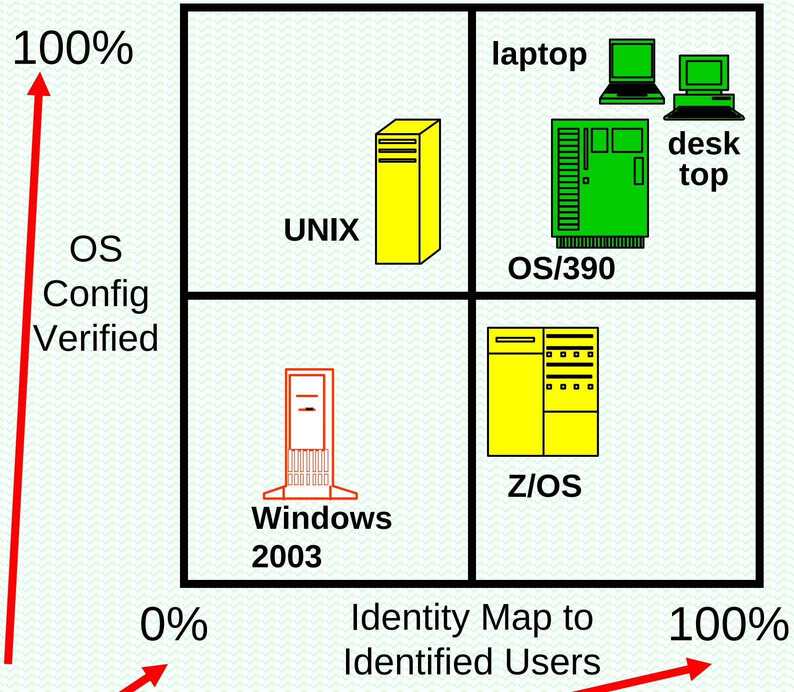
Total Population

Population in compliance

Facilitates comparison between different sets of management

Compare: Automation

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

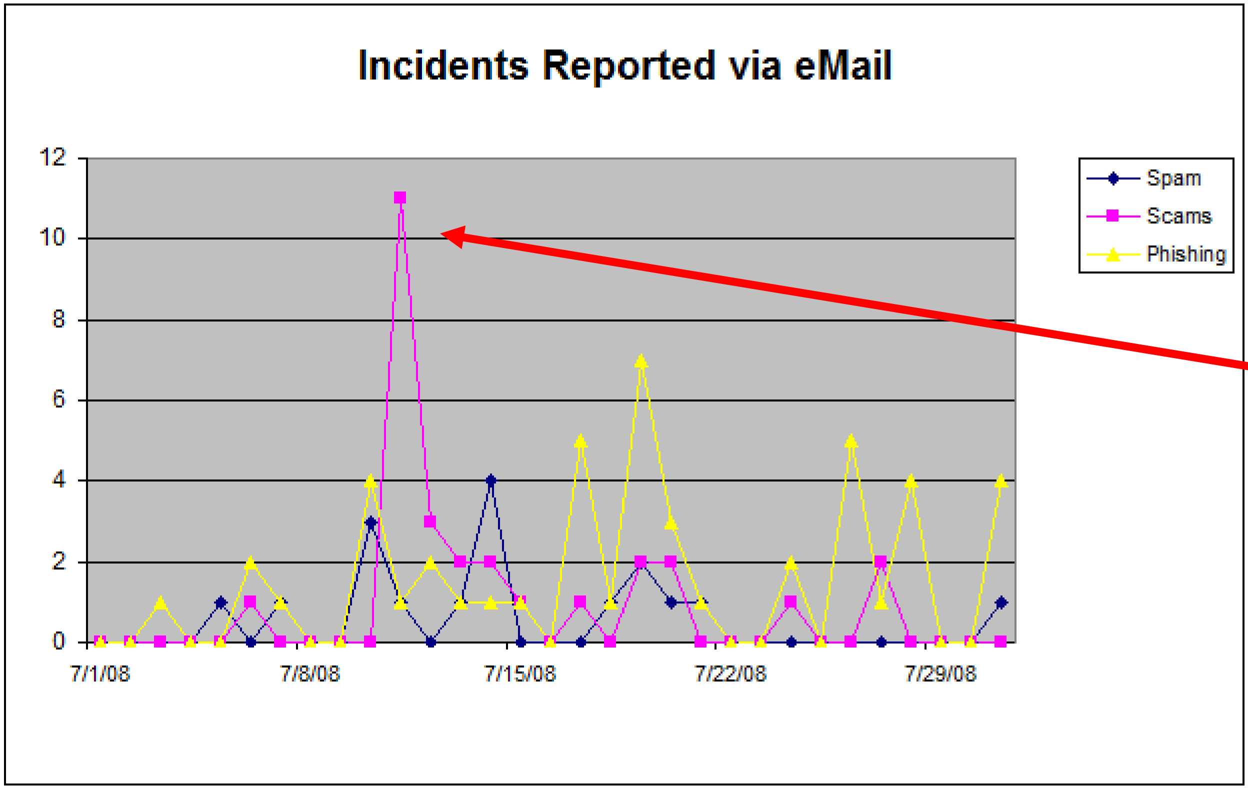


Machine population

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

Compare: Trends

Often used to depict activity beyond control of management



Incidents Reported via eMail

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

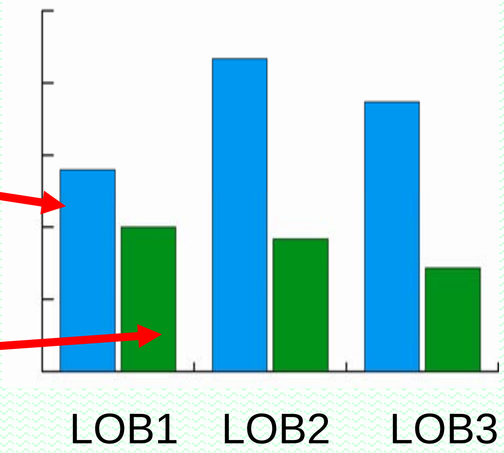
Contrast: Focus

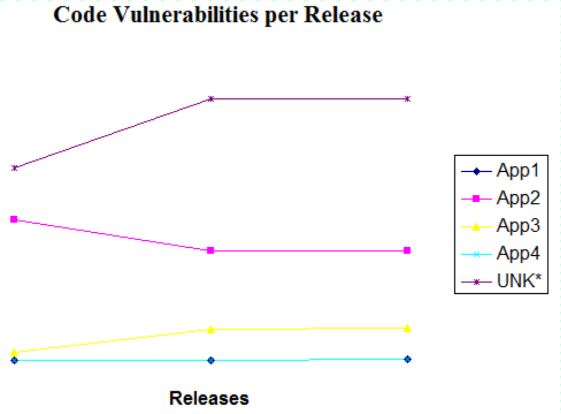
Risk Security

Coverage vs Quality

Total Number of applications

Total applications scanned for code vulnerabilities



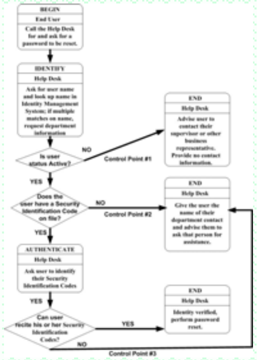


Focus on quality of security results in this type of report

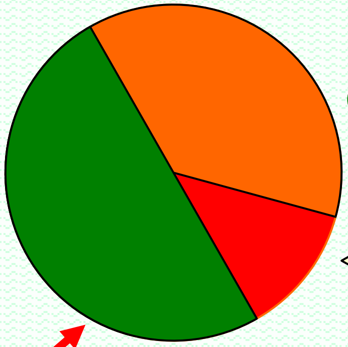
Confidence in totals comes with aggregation rather than collection.

Contrast: Basis

Risk *Policy* *vs* Security *Process*


BEGIN
End User
Call the Help Desk for and ask for a password to be reset.
IDENTIFY
Help Desk
Ask for user name and look up name in Identity Management System; if multiple matches on name, request department information
Is user status Active?
NO
Control Point #1
END
Help Desk
Advise user to contact their supervisor or other business representative. Provide no contact information.
YES
Does the user have a Security Identification Code on file?
NO
Control Point #2
END
Help Desk
Give the user the name of their department contact and advise them to ask that person for assistance.
YES
AUTHENTICATE
Help Desk
Ask user to identify their Security Identification Codes
YES
Can user recite his or her Security Identification Codes?
YES
END
Help Desk
Identity verified, perform password reset.
NO
Control Point #3

Population with authorized exceptions to compliance

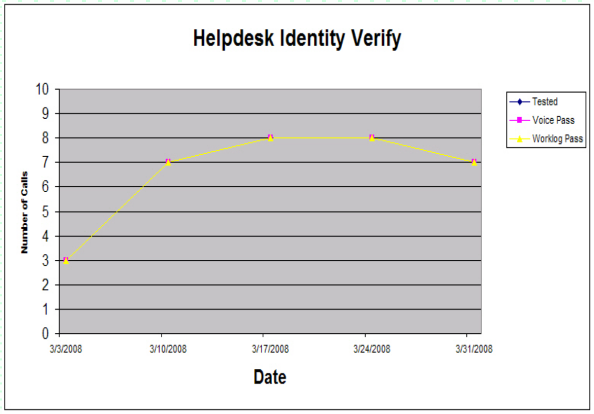


Population not in compliance

Population in compliance

Security managers look for correlation.

Control points from process directly correlated to measured activity.

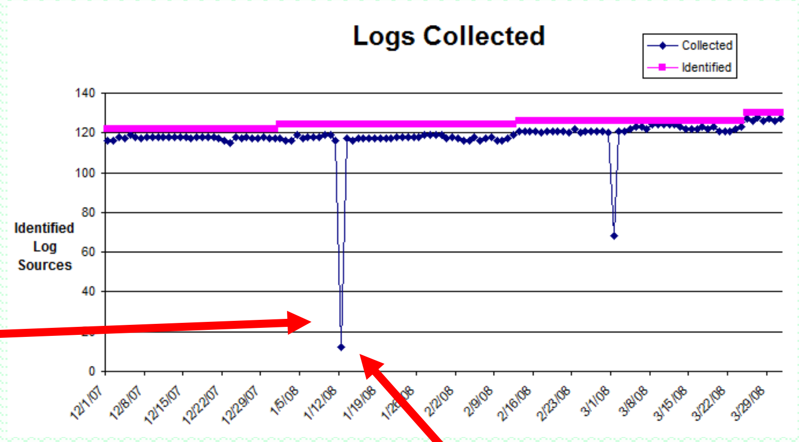


Contrast: Reliance

Risk Security

Explanations vs Accountability

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



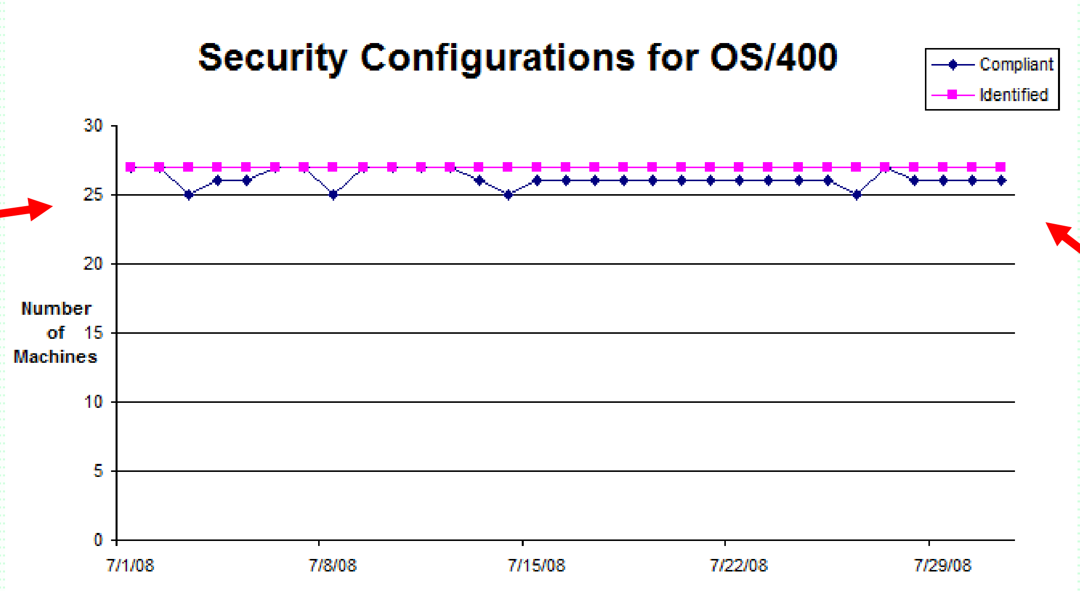
Where there is a process in place designed to maintain the metrics, there should be accountability for poor results.

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

Contrast: Reflects

Risk *Assessment* *vs* Security *Implementation*

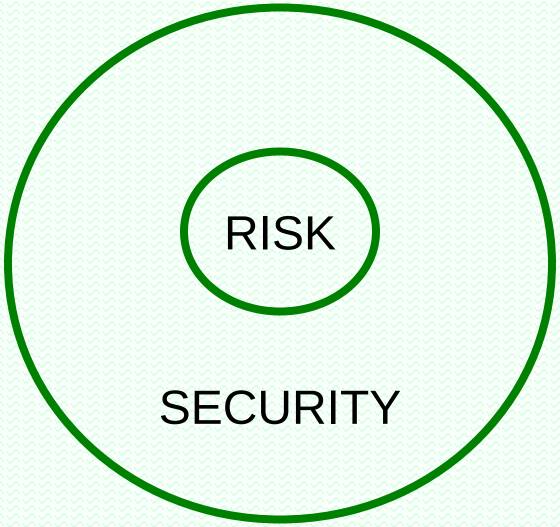
Risk manager see no dramatic changes



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