Global Information Security (GIS) Metrics

Enterprise plans and lessons learned

Tuesday 29 July 2008, Metricon 3.0

Caroline Wong, CISSP
Global Information Security (GIS) Chief of Staff & Mgr, Metrics
Li Liu, PhD, Lead Metrics Engineer
Dave Cullinane, CPP, CISSP, CISO & VP

eBay

Founded in 1995, eBay Inc. connects hundreds of millions of people around the world every day, empowering them to explore new opportunities and innovate together. eBay Inc. does this by providing the Internet platforms of choice for global commerce, payments and communications. Since its inception, eBay Inc. has expanded to include some of the strongest brands in the world, including eBay, PayPal, Skype, StubHub, Shopping.com, and others. eBay Inc. is headquartered in San Jose, California.

At any given time, there are approximately <u>112.3 million listings worldwide</u>, and approximately <u>7.1 million listings</u> are added per day.

A pair of shoes sells every
7 seconds

A cell phone sells every
7 seconds

A car sells every
56 seconds

Trust is at the core of every successful eBay transaction

Metrics Vision

Track and assess metrics to ensure that we are effectively meeting the security needs of the corporation, managing risk and assuring ROI.

Program management

- Project prioritization & success criteria
- Metrics drive roadmap, resourcing, budget
- Data informs GIS mgmt for decision-making
- Feedback loop for continuous improvement

Drive organizational change

- Appropriate ownership & accountability for security issues
- VP's receive regular status reports showing KRI's and KPI's that are relevant to their BU
- VP's understand reports and know what they must do for remediation

Benchmarking

- Compare eBay MP risk levels to external risk levels

Operational / tactical decision making

- Support GIS teams for day to day decision-making

Metrics Vision

Track and assess metrics to ensure that we are effectively meeting the security needs of the corporation, managing risk and assuring ROI.

Program management

- Project prioritization & success criteria
- Metrics drive roadmap, resourcing, budget
- Data informs GIS mgmt for decision-making
- Feedback loop for continuous improvement

Drive organizational change

- Appropriate ownership & accountability for security issues
- VP's receive regular status reports showing KRI's and KPI's that are relevant to their BU
- VP's understand reports and know what they must do for remediation

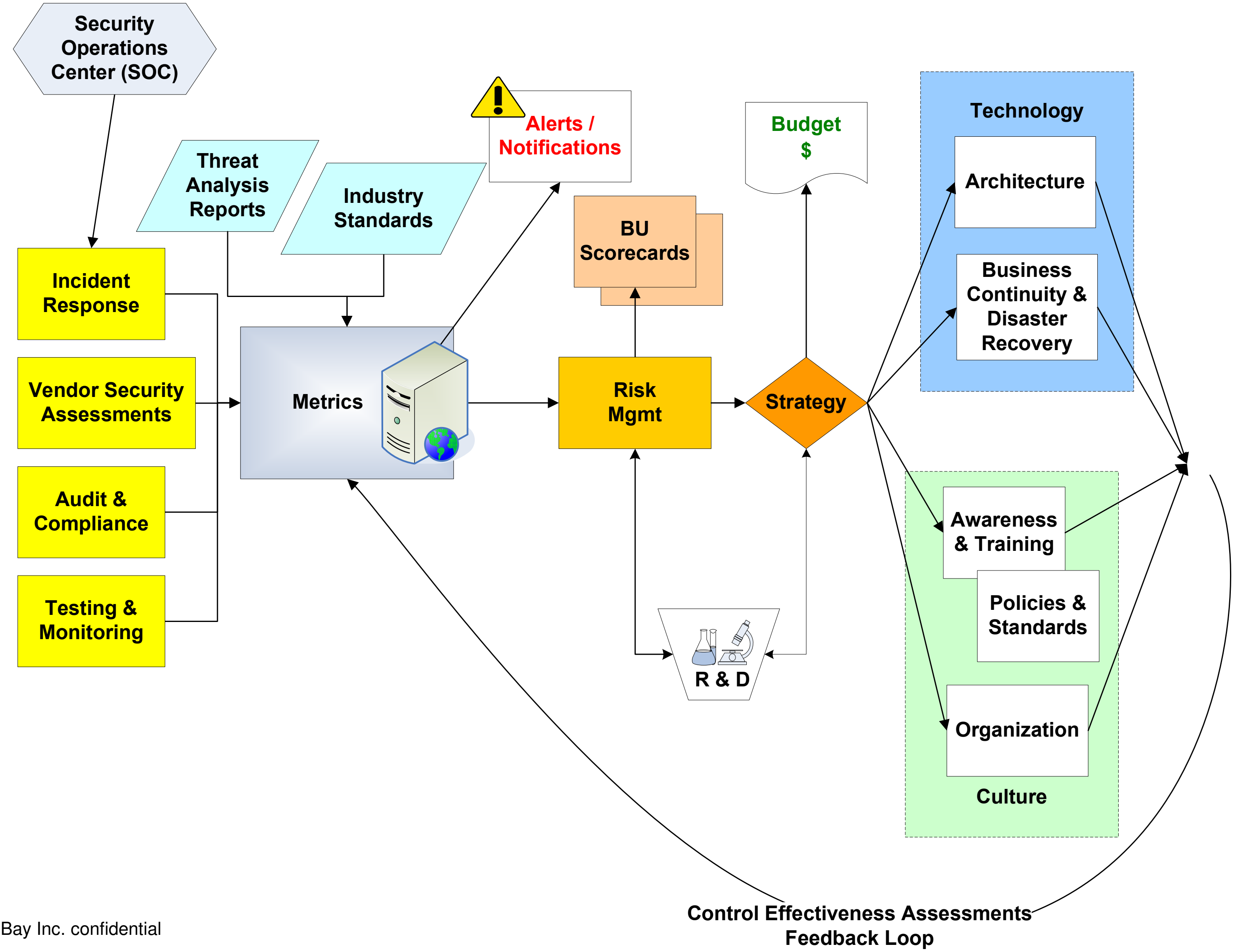
Benchmarking

- Compare eBay MP risk levels to external risk levels

Operational / tactical decision making

- Support GIS teams for day to day decision-making

Predictive Model Feedback Loop



Security Operations Center (SOC)

Threat Analysis Reports

Industry Standards

Alerts / Notifications

BU Scorecards

Budget $

Technology

Architecture

Business Continuity & Disaster Recovery

Incident Response

Vendor Security Assessments

Audit & Compliance

Testing & Monitoring

Metrics

Risk Mgmt

Strategy

Awareness & Training

Policies & Standards

Organization

Culture

R & D

Control Effectiveness Assessments Feedback Loop

eBay Metrics Program

Assumptions

- Security is a means to an end (protect the business)
- Metrics are also a means to an end (enable risk mgmt)
- Metrics serve security professionals, not the other way around (we are smarter than the numbers)
- **Don't spend too long— go for most meaning with least effort**

Approach

- Top down (what do you want to know) and bottom up (data you already have)
- Data can be business based or technology based
- Identify Key Risk Indicators (measure current state) and Key Performance Indicators (define desired state)
- Automate as much as possible (again, most meaning, least effort)

What data?

- There is likely a common set of generic technical metrics; business metrics will depend on business model & processes
- Common tech metrics include incidents, patching, losses, compliance, vulnerabilities

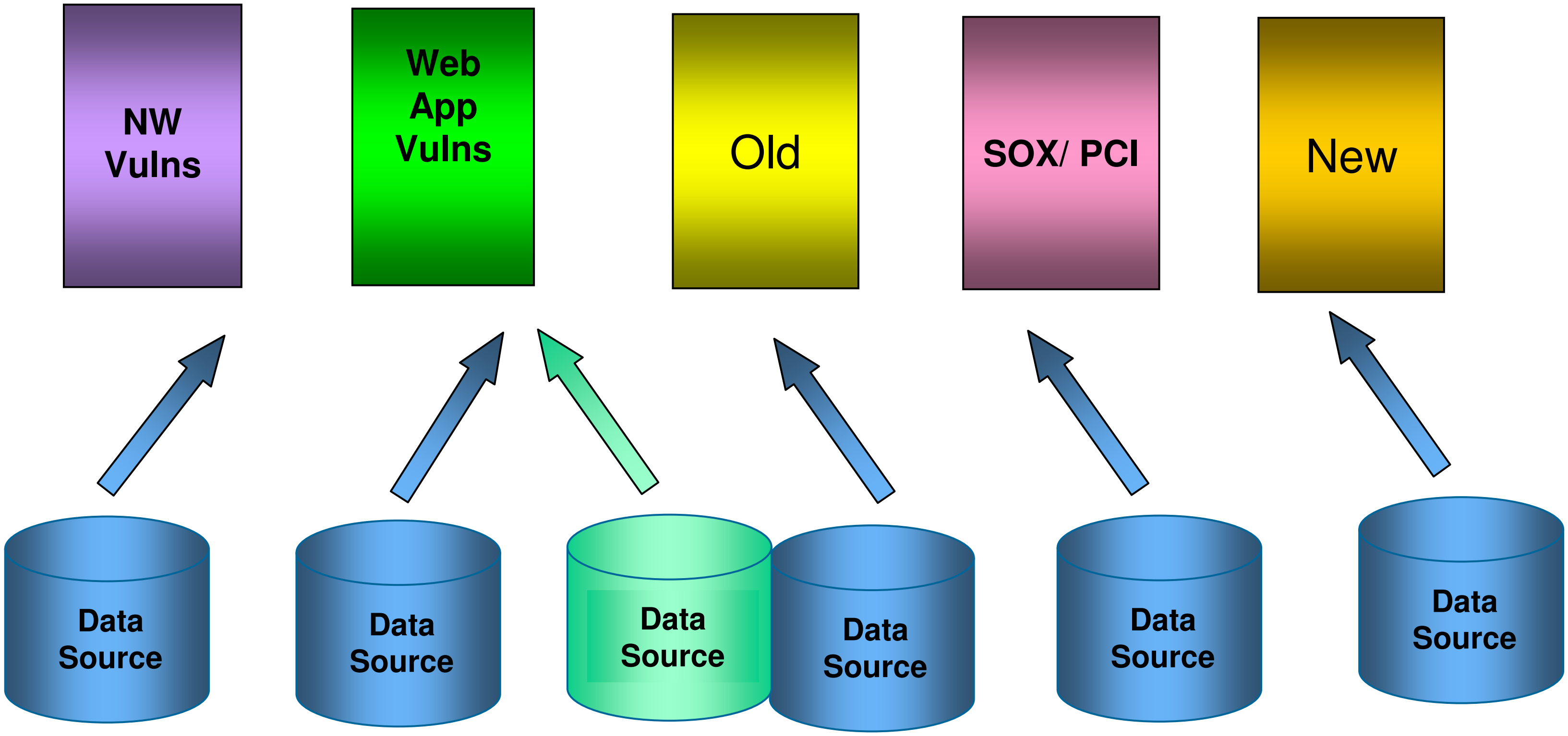
Changing Environment Requires Flexibility

Constantly changing environment - new tools, priorities, data formats

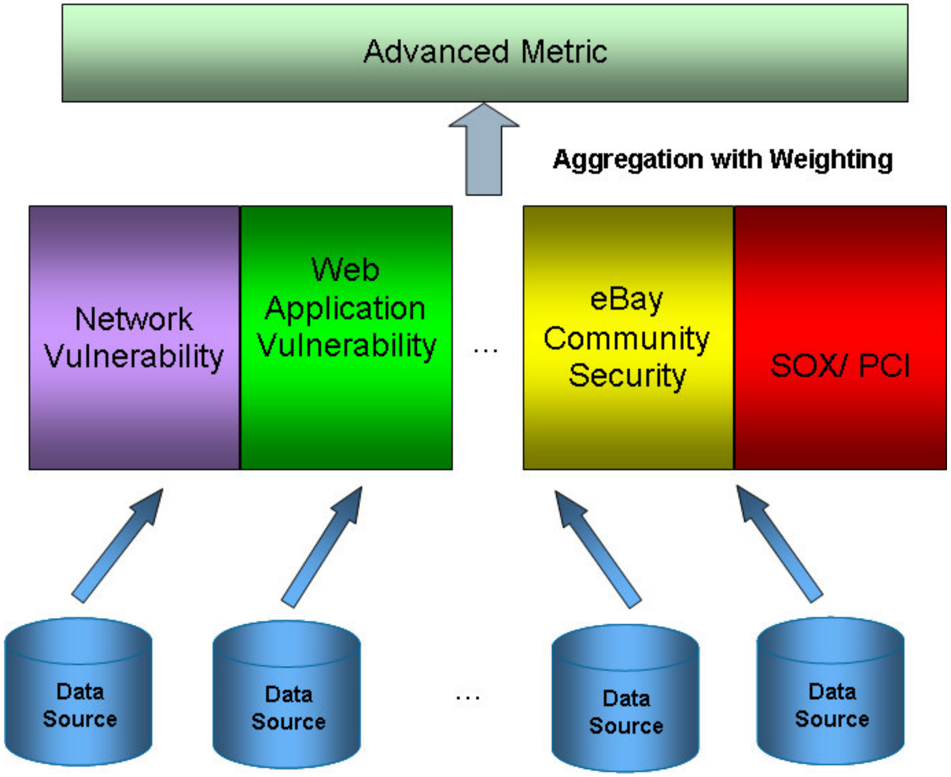
System must be flexible and dynamic

Changing Environment Requires Flexibility

Process to add or update data sources must be quick and simple



Risk Ratings



Normalization

- How to normalize the row data?
- How to read the data?

Aggregation

- Same category may have different data sources.
- How to combine the data from different categories?

Risk ratings

- How to assign the proper weight to different data sources in same category? In different categories?
- No rules to follow; different businesses require different risk ratings

Questions?

Any questions, please contact

- Caroline Wong at carwong@ebay.com

- Li Liu at liiliu@ebay.com