

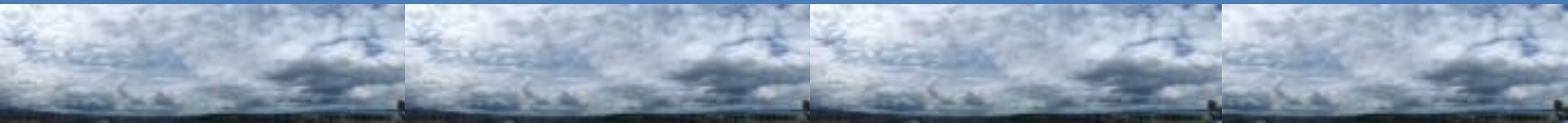


# Cloud Security Alliance: Metrics Working Group

Caroline Wong, eBay  
Betsy Nichols, Plexlogic  
Lynn Terwoerds, SafeMashups

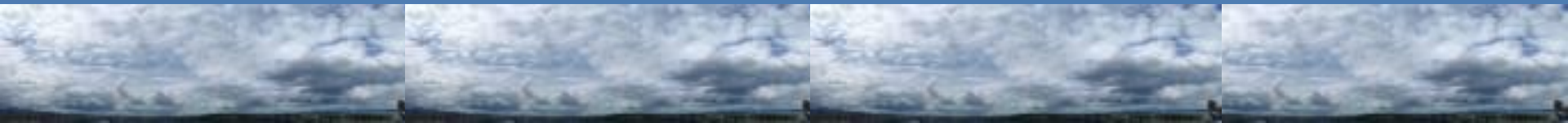
# Agenda

- Cloud Security Alliance
- Current Conditions
- CSA Cloud Metrics Working Group
- Progress Report
- MetricsCenter Catalog: Candidate Metrics
- Call to Action



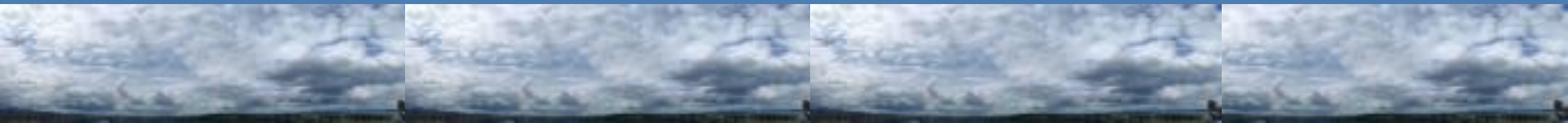
# Current Conditions

- Cloud specific security metrics are either non-existent or early stage
- Since metrics are specific and cloud computing is still evolving, the working group must establish a cycle of review and revision
- The value proposition of the metrics working group is twofold
  1. It enhances and supports the CSA guidance
  2. The working group will publish its metrics in an open format which allows for comment, revision history and eventually consumption by the entire CSA (and potentially other) community.



# Focus

- 3 of the 13 CSA Domains
  - Encryption & Key Management
  - Governance & Enterprise Risk Management
  - Application Security
- Define within each domain, areas of concentration based on expertise in the working group
- Examples will be shown in demo



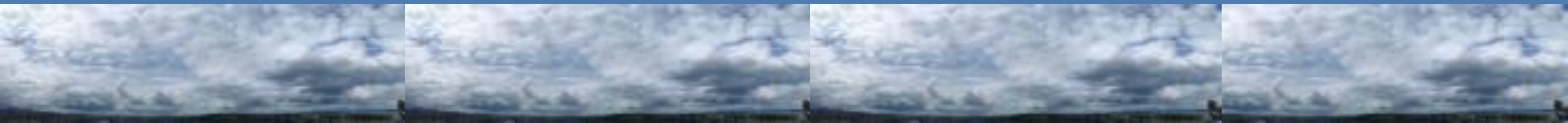
# Outputs

- Leverage the Metrics Center catalog
- Each domain area has a lead and we publish based on the following lifecycle



# Coordination with Other Security Metrics Efforts

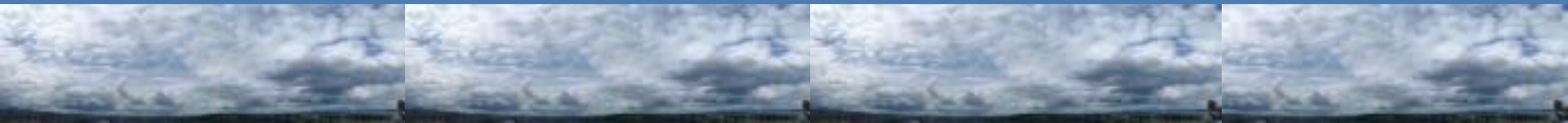
- Metrics Center catalog is a central repository for security metrics
- Schema allows for cross referencing
- Commitment to attribution
- Coordination with Center for Internet Security



# Progress to Date

- Active working group with participants for each of the 3 CSA domains

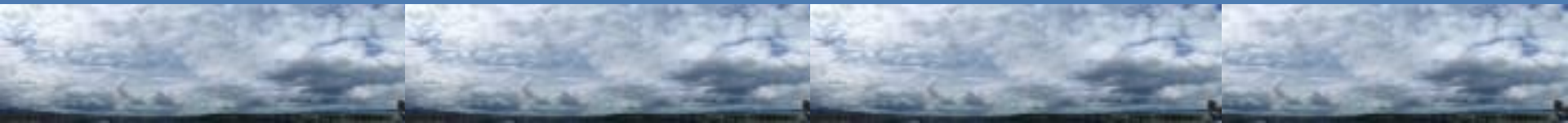
<b>Lynn Terwoerds</b>	Chair, Co-founder	<b>Jeff Lowder</b>	Application security
<b>Betsy Nichols</b>	Co-founder	<b>Martin Rues</b>	Application security
<b>Caroline Wong</b>	Co-founder	<b>Hemma Prafullchandra</b>	Gov & Risk mgmt
<b>Tara Darbyshire</b>	Co-founder	<b>Dan Crisp</b>	Gov & Risk mgmt
<b>Tim Mather</b>	Encryption/key mgmt	<b>Steph Spence</b>	Gov & Risk mgmt
<b>Eric Ashdown</b>	Encryption/key mgmt	<b>Matt Broda</b>	CAM rep
<b>Katie Moussouris</b>	Application security		
<b>Ashish Larivee</b>	Application security		



# Coordination with CSA Related Initiatives

- Control Matrix working group (CSA)
- CloudAudit (formerly known as A6)
- Common Assurance Metric (ENISA)
- Trusted Cloud Initiative (CSA)
- Center for Internet Security

*Common denominator for all of these related initiatives is coordination and collaboration through the Cloud Security Alliance*



# Metrics Center Demo

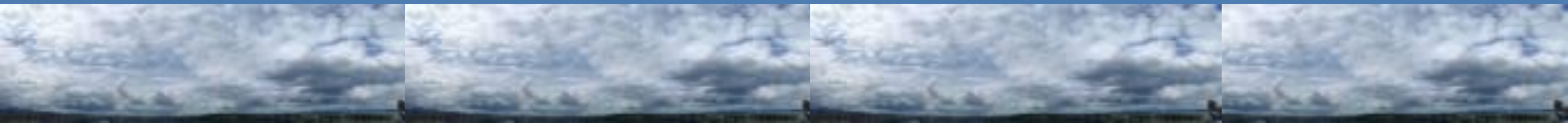
The screenshot shows a Windows Internet Explorer browser window displaying the Metrics Center website. The address bar shows the URL <https://csa.metricscenter.net/>. The browser's Favorites bar includes links for Virtuosì, CSA Metrics, GoToMtg, CNN, and Live. The website header features the MetricsCenter logo and a navigation menu with links for Home, Catalog, Dashboards, Resources, Free Trial, and About. A main banner image shows two people on a sailboat with 'Cambrils' and 'NEELPRYDE' written on the hull. A dark overlay on the right side of the banner contains a list of features:

- Anonymously Submit Data
- Receive Custom Dashboards
- Join a Trusted Community
- Compare Metrics With Peers

The footer of the website contains the following text: (c) 2008-2010 PlexLogic, LLC | This site is powered by MetricsCenter(tm) V 0.0( #198 Tue Jan 26 00:27:35 EST 2010 ) | Joomla! (r) v.1.5.15 | Terms of Use | Privacy Policy. The Windows taskbar at the bottom shows the system tray with the time 12:16 PM and date 2/18/2010, and the taskbar includes icons for Internet Explorer, Mail, and other applications.

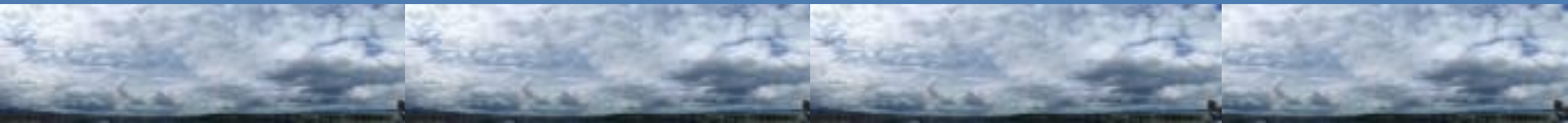
# MetricsCenter Services

- Design Phase
  - Catalog
  - Metrics Definition Framework (Metric XML)
- Implementation Phase
  - Data Ingestion
  - Metric Compute Logic
  - Visualization and Reporting
- Production Phase
  - Scheduling and Workflow Management
  - Dashboards + Collaboration



# Catalog Services

- Design: metrics, datasets, dimensions, contexts
- Centralized catalog
- “Common denominator” for
  - Metric specification
  - Collaboration
  - Documentation of design rationale and progress
- Versioning, Comments, Community Forum
- Comments, Community Forum, Rating, RSS Feeds
- Context Mapping
- Licensing
- Sharing via open XML Schema



New

Contexts

- Cloud Security Alliance
  - 1. Cloud Computing Architectural Framework
  - 2. Governance and Enterprise Risk Management
  - 3. Legal and Electronic Discovery
  - 4. Compliance and Audit
  - 5. Information Lifecycle Management
  - 6. Portability and Interoperability
  - 7. Traditional Security, Business Continuity, ar
  - 8. Data Center Operations
  - 9. Incident Response, Notification and Remed
  - 10. Application Security
    - A. Providers
    - B. Developers
    - C. Consumers
  - Application Migration to Cloud
  - 11. Encryption and Key Management
  - 12. Identity and Access Management
  - 13. Virtualization
- BSIMM
- Public Data Source Metrics
- PCI DSS v1.2
- NIST Metric Type
- NIST SP800-53 Controls
- ISO/IEC 27002
- Computer Information Security Working Group (
- CIS Consensus Metrics
- Enterprise Metrics
- Orphans

Search Results

Advanced Search

2. Governance and Enterpr... ALL enter search

CloudDataClassificationCoverage

Consumers of cloud services (IaaS, PaaS, SaaS) share control of their information assets with a cloud service provider, and as such need to govern the ... 02/16/2010(LATEST VERSION)

DataRemanenceReview

This metric attempts to address compliance issues around secure disposal of assets and complete removal of data from storage media. Look at the CSA C... 02/03/2010(LATEST VERSION)

+ New ▾

## Contexts

- Cloud Security Alliance
  - 1. Cloud Computing Architectural Framework
  - 2. Governance and Enterprise Risk Management
  - 3. Legal and Electronic Discovery
  - 4. Compliance and Audit
  - 5. Information Lifecycle Management
  - 6. Portability and Interoperability
  - 7. Traditional Security, Business Continuity, and Disaster Recovery
  - 8. Data Center Operations
  - 9. Incident Response, Notification and Remediation
  - 10. Application Security
  - 11. Encryption and Key Management
  - 12. Identity and Access Management
  - 13. Virtualization
- BSIMM
- Public Data Source Metrics
- PCI DSS v1.2
- NIST Metric Type

## Search Results

### Advanced Search

2. Governance and Enterpr... ALL enter search

### CloudDataClassificationCoverage

Consumer information (SaaS, PaaS, SaaS) share control of their service provider, and as such need to govern (VERSION)

### DataRe

This metri assets and C... 02/03 compliance issues around secure disposal of data from storage media. Look at the CSA (SION)

- Inspect
- Edit All
- Clone
- RSS Feed
- Export
- Export All
- Delete
- Delete All

+ New

% info assets classified and labelled

**Name:** % info assets classified and lab **Version:** LATEST

**Owner:** lterwoerds@gmail.com **Group Owner:** csa

**Rating:** ★★★★★ **Views:** 6

**Created:** 2010-01-27 **Updated:** 2010-02-22

**Title:** CloudDataClassificationCoverage

**Status:** Draft

**Audience:** Management

**Units of Measure:** % of all business critical cloud bound data

**Targets:** Since the metric relates to business critical data and regulated data (not all data sent to a cloud service provider), the target should be in line with your company's data governance board or equivalent industry benchmark.

**Description:** Consumers of cloud services (IaaS, PaaS, SaaS) share control of their information assets with a cloud service provider, and as such need to govern the data. In the IaaS model, there is a higher degree of shared responsibility, however with PaaS and especially in SaaS, the consumer will have limited view where the data flows and how it is being processed and stored.

This metric was developed based on best practices and existing security guidance: Complete Guide to Security and Privacy Metrics, Debra S. Hermann  
Cloud Security and Privacy, Tim Mather, Subra Kumaraswamy, Shahed Latif  
CSA Controls Matrix working group "Cloud Security Controls Matrix", DG-03

**Objective:** This metric is meant ensure consumers of cloud services know what critical data is being sent outside the enterprise, the relative value of that data to the business and that the data has been appropriately marked. This metric should assist the cloud consumer in making risk based information security decisions, weighing the relative value of the data assets which are moving from the traditional enterprise to the cloud service provider. The business value of this metric is only realized if the organization can make more informed risk-based decisions about their data, such as strengthening the security schedule in a vendor contract to reflect the value of the data now being sent outside the company.

Comments

- 02/02/2010 **Lynn**
- 02/02/2010 **Lynn**  
This is a test comment
- 02/22/2010 **ean**
- 02/22/2010 **ean**  
What data classification tools exist and what sort of data can they provide? Can this metric be computed based upon data typically provided by tools?

# Metric XML Example

```
<?xml version="1.0" encoding="UTF-8" ?>
<definitions xsi:schemaLocation="file://home/ean/workspace/MetricXML/metric.xsd metric.xsd" mc-version="1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="file://home/ean/workspace/MetricXML/metric.xsd">
  <!-- id: 234458 v: 0
  -->
  - <definition audience="Management" create-date="2010-01-27 12:14:58" name="% info assets classified and labelled" last-updated="2010-02-22
    15:52:46" status="Draft">
    <title>CloudDataClassificationCoverage</title>
    <uom>% of all business critical cloud bound data</uom>
    <targets>Since the metric relates to business critical data and regulated data (not all data sent to a cloud service provider), the target
      should be in line with your company\'s data governance board or equivalent industry benchmark.</targets>
    <description>Consumers of cloud services (IaaS, PaaS, SaaS) share control of their information assets with a cloud service provider, and as
      such need to govern the data. In the IaaS model, there is a higher degree of shared responsibility, however with PaaS and especially in
      SaaS, the consumer will have limited view where the data flows and how it is being processed and stored. This metric was developed
      based on best practices and existing security guidance: Complete Guide to Security and Privacy Metrics, Debra S. Hermann Cloud Security
      and Privacy, Tim Mather, Subra Kumaraswamy, Shahed Latif CSA Controls Matrix working group \\'Cloud Security Controls Matrix\\', DG-
      03</description>
    <objective>This metric is meant ensure consumers of cloud services know what critical data is being sent outside the enterprise, the relative
      value of that data to the business and that the data has been appropriately marked. This metric should assist the cloud consumer in
      making risk based information security decisions, weighing the relative value of the data assets which are moving from the traditional
      enterprise to the cloud service provider. The business value of this metric is only realized if the organization can make more informed risk-
      based decisions about their data, such as strengthening the security schedule in a vendor contract to reflect the value of the data now
      being sent outside the company.</objective>
    <usage>I envision the metric employed to support terms of a security schedule as part of a service contract with a cloud service provider. In
      addition, the cloud consumer should become quickly aware if they are blissfully unaware or do not have management of assets leaving
      their company and being processed, moved and stored by a cloud service provider.</usage>
    <automation><i>I need help with a discussion about any data classification tools. The important part is to remain vendor neutral and figure
      out how to keep this up to date.</i></automation>
    <frequency>Quarterly or as needed</frequency>
    <sources>An inventory of any business critical data must be documented before moving the data and/or application to the cloud service
      provider. Indications of gaps include the following: - Applications lacking business and/or technical owners - Unstructured data - Business
      applications which have been informally identified as business critical but not properly documented or inventoried - Data and applications
      coming from a recent acquisition where business integration is not complete - Data and applications coming from a business unit
      disconnected from centralized GRC function and information security, or generally functioning independent of the business and IT
      functions engaged with the cloud service provider.</sources>
    <calculation />
    <methodology />
    <limitations>This metric assumes enterprises already have a data classification scheme and are implementing it for business critical data.
      This metric also assumes, business critical or sensitive data is not widely distributed in the form of unstructured data and therefore not
      tracked prior to moving to cloud computing.</limitations>
```

# Call to Action

- Join the CSA Cloud Metrics Working Group
- More info at [http://groups.google.com/group/csa\\_metrics](http://groups.google.com/group/csa_metrics)
- Create, review and/or comment on the cloud security metrics
- Sign up for the RSS feed

