Security Metrics

Establishing unambiguous and logically defensible security metrics

Steven Piliero
CSO
The Center for Internet Security

the CENTER for INTERNET SECURITY

The Center for Internet Security (CIS)

- **Formed** - October 2000
  - As a not-for-profit public-private partnership
- **The mission** – produce security guidance to:
  - Help organizations **measurably reduce risk**
  - Equip IT buyers with **purchasing leverage** so they can buy systems with **security built-in**
  - Support the higher level standards/regulations with unambiguous **operational-level "how-to" detail**
- **The method**
  - Security benchmarks **built by consensus teams** of security experts
- **The use** – downloaded **over 1,000,000 times / year**

the CENTER for INTERNET SECURITY

Agenda

- **CIS Security Metrics Initiative**
  - Overview
  - Objective and Goals
  - Consensus team
- **Security Metrics**
  - The Challenge
  - What is a metric?
  - Business outcomes – measure the right things
  - Examples
- **How to participate**
- **Summary**
- **Questions**

Current Reality

- A focus on compliance with practices / processes with inadequate attention to outcomes
- Security investment decisions made on an intuitive basis
- Lack an effective feedback / learning loop
- Lack of adequate information sharing
- The result is an independent, metric framework to define, collect and analyze data on security outcomes and process benefits.

What's Missing?

- A widely accepted, overarching definition of success
- Consensus Security Metrics
- A comprehensive **feedback learning** mechanism for continuous improvement

Essential Value Proposition

- “Align Risk to Organization Risk Tolerance

- Create Operational Efficiencies”

CIS Security Metrics Abstract

- Organizations struggle to make cost-effective security investment decisions;
- Information Security Professionals lack widely accepted and unambiguous metrics for decision support.
- CIS established a consensus team of industry experts to address this need.
- The result is an independent, metric framework to define, collect and analyze data on security outcomes and process benefits.

the CENTER for INTERNET SECURITY

Security Metrics Initiative

- sponsored by the Center for Internet Security
- proven track record in security guidance
- community driven consensus group
- establish practical approaches to security management.

✓ Initial Security Metrics selected (Milestone 1)
✓ Complete draft definition Metrics (Milestone 2)
✓ Publish initial Security Metrics (Milestone 3)

the CENTER for INTERNET SECURITY

Objective and Goals

- Achieve community consensus on a small number of security outcome metrics.

1. Establish unambiguous and widely accepted security metrics

2. Provide mechanisms for organizations to benchmark and effectively communicate performance.

3. Establish widely understood and proven correlation of security practices and security performance.

Scope and Purpose

- Create standard metrics
  - To **reduce the impact of incidents** that interfere with critical enterprise functions
  - To support better security investment decisions
- Facilitate future inter-enterprise benchmarking
  - For correlation of practices with outcomes
  - For best practice discovery

Consensus team members

- **Corporations and Organizations**
  - Small – Fortune 50 organizations, non-profit and commercial, many industry verticals, **especially banking and financial**
- **Industry Experts**
  - Mathematicians, statisticians, actuaries, CISO's, security managers
- **Government**
  - Federal, state, and local
- **Vendors**
  - Security product, solution and consulting firms
- **Universities and Researchers**
  - Well know institutions that specialize in information security

the CENTER for INTERNET SECURITY

The Challenge

- ‘How secure are we?
- Are we better off than this time last year?
- Are we spending the right amount of $$?
- How do we compare to our peers?’[1]

- Can we unambiguously communicate performance in terms relevant to customers and our business?

What is a metric?

- A standard of measurement[2] that facilitates the quantification of some particular characteristic[3]
- Enables repeatable measurement
- Facilitates decision making
- Examples from other industries:
  - Profit Margin[4,5] - (finance & accounting)
  - Transit time[6]- (transportation & logistics)
  - Cost per click[7,8,9] – (advertising & marketing)
  - Customer Satisfaction[10,11] – (business & marketing)
  - Post Surgical Infection Rate[12] – (Healthcare & Insurance)

Metric vs KPI

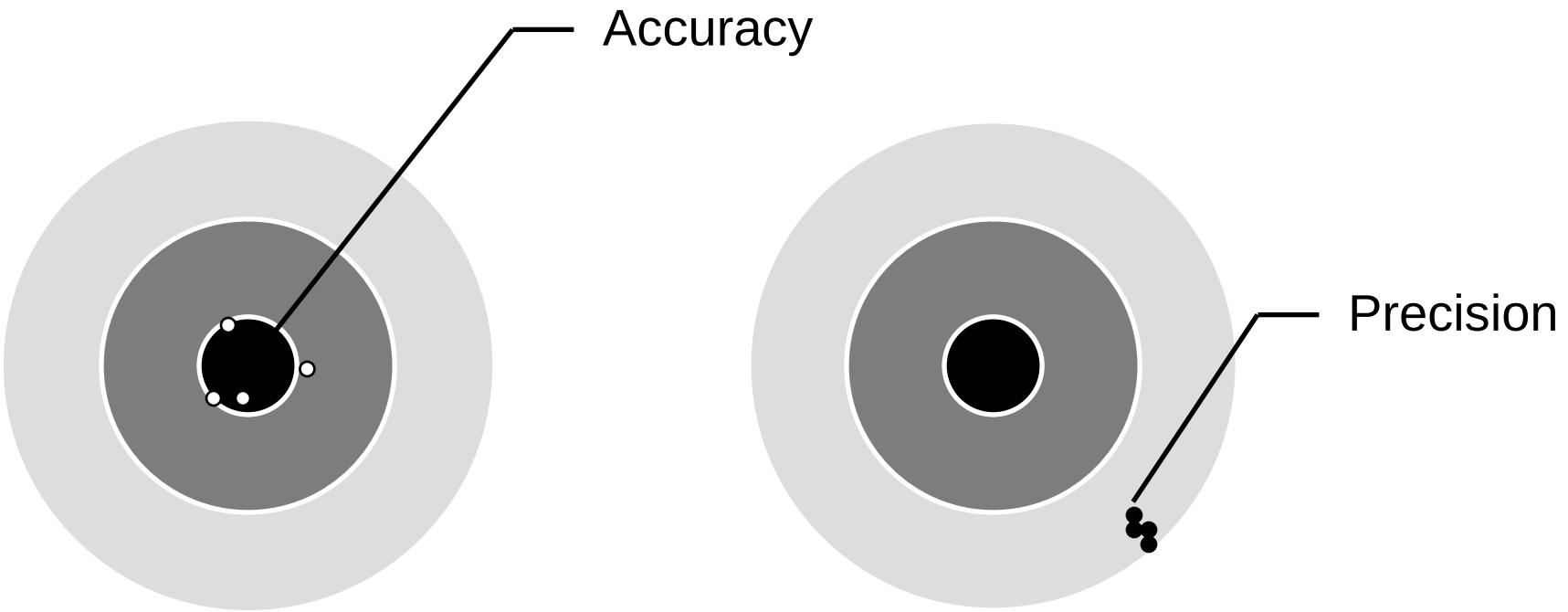
- Sound key performance indicators (KPI's) necessitate that we:
  - First have good metrics, based on sound measures, for making decisions under conditions of uncertainty and
  - Second we establish appropriate thresholds

Qualitative and Quantitative Data

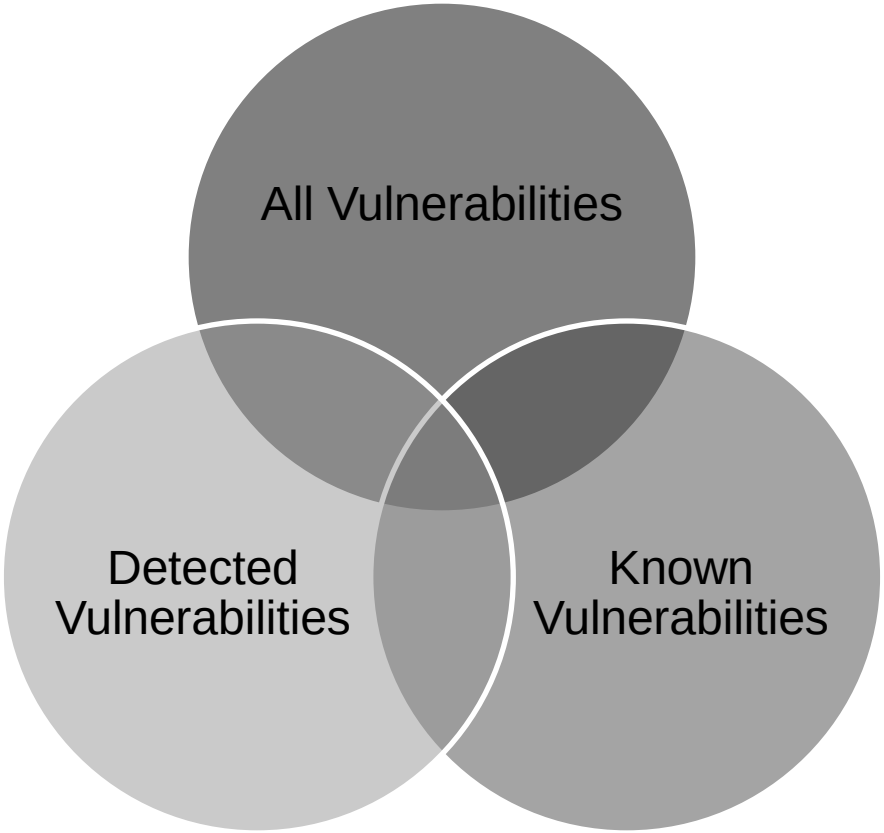
- Quantitative Data
  - Interval - origin is a meaningful number
  - Ratio

- Qualitative Data
  - Nominal – can’t be ordered
  - Ordinal – can be meaningfully ordered

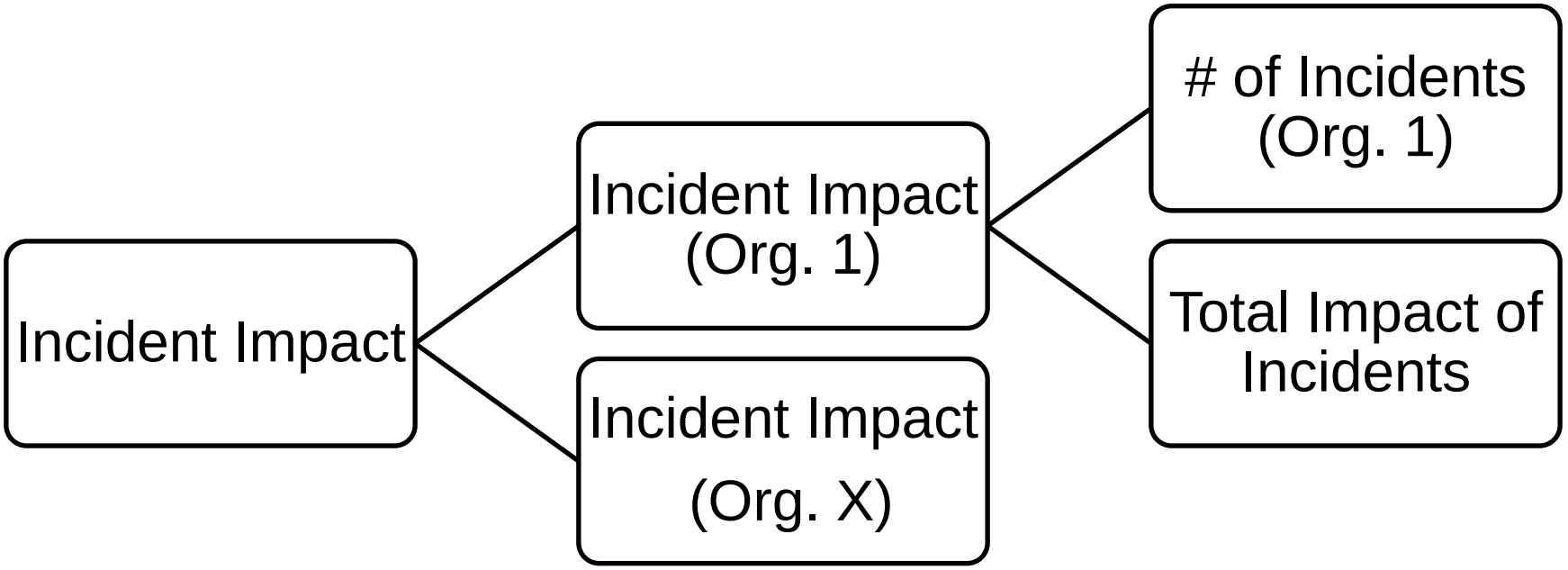
Accuracy & Precision



Context and Meaning



Dimensions, Aggregates & Primitives



Business Outcomes

Measure the right things

- (Step 1) Business outcomes
  - **Performance Metrics[13]** – how you are doing
  - Screening Test(s)
  - Inspires drill-down questions by seeding thinking process

- (Step 2) Internal business processes & practices
  - **Diagnostic Metrics[13]** – ascertain why
  - An unacceptable value of an outcome metric will invariably suggest that the organizational process that produced the outcome is in need of improvement

Example: Online Banking

- How do customers measure success?
  - ‘My transactions are authorized by me
  - My information is safe
  - My information is secure
  - My information is available’[14]
- Key Assurances:
  - ‘My data is private;
  - My identity cannot be compromised;
  - The resources I require are secure and available; and
  - I understand my role in building a secure environment.’[14]

Business Functions Covered

- Incident Management
- Financial
- Change Management
- Vulnerability Management
- Patch Management
- Software Security

the CENTER for INTERNET SECURITY

Sample of CIS Consensus Metrics

- Security Incidents
  - Rate of Security Incidents
  - Mean-Time-Between-Security Incidents
  - Mean-Time-To-Incident Discovery (MTTID)
  - Mean-Time-To-Incident Recovery (MTTIR)
  - Incident Impact (Draft)
  - % of Incidents Detected by Internal Controls (Draft)

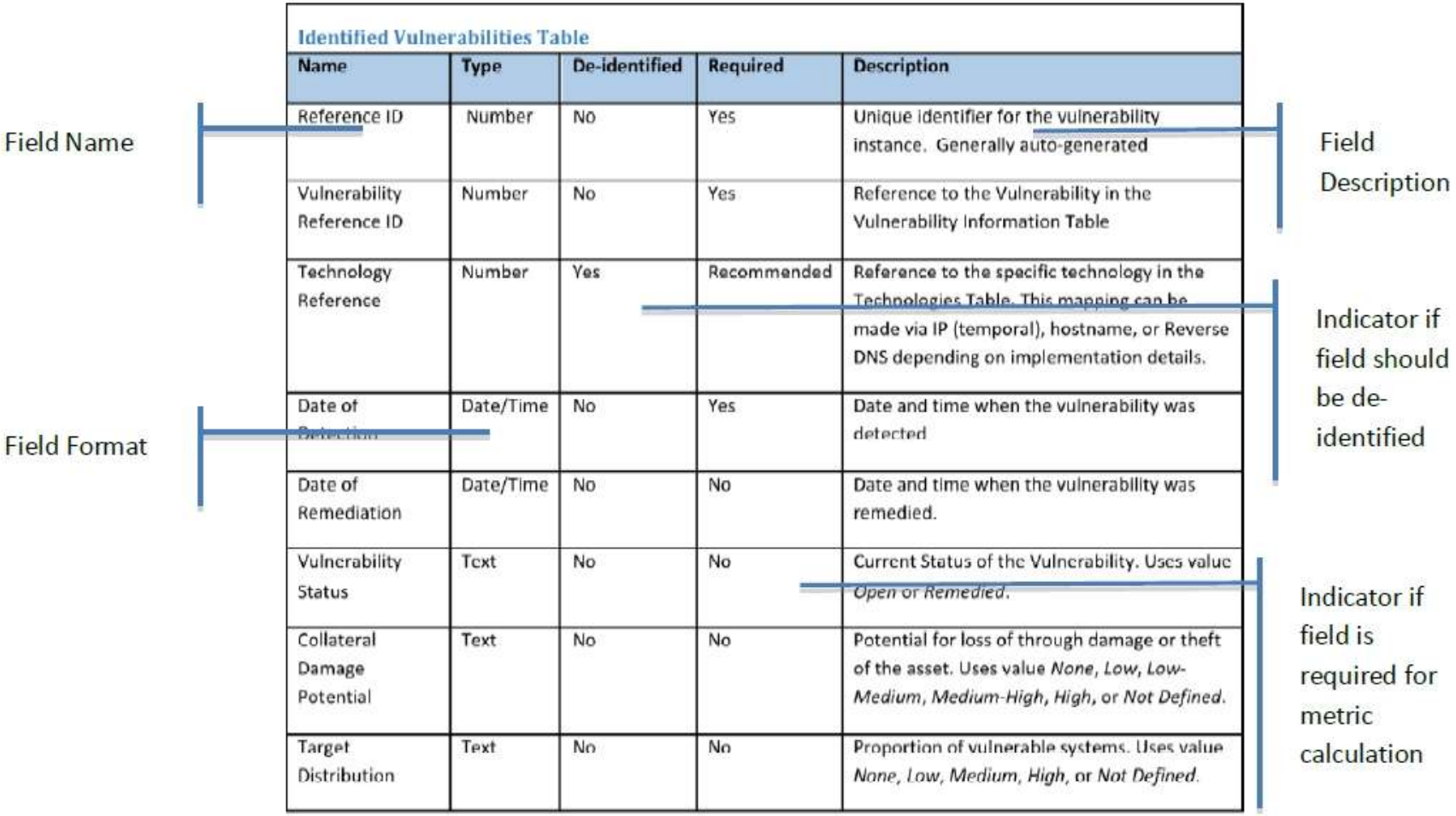
Consensus Metric Definitions

1. Pose business questions (goal)
2. Create Data Set Definition of readily available information to answer business questions
3. Develop unambiguous metrics derived from Data Set.
   - Title
   - Description
   - Objective
   - Usage
   - References
   - Calculation and Visualization…….

Example: Business Questions

- Is there a sustained reduction of security incident impact over time?
- How well do we detect, accurately identify, handle and recover from security incidents?

Example: Data Set



Identified Vulnerabilities Table

Name	Type	De-identified	Required	Description
Reference ID	Number	No	Yes	Unique identifier for the vulnerability instance. Generally auto-generated
Vulnerability Reference ID	Number	No	Yes	Reference to the Vulnerability in the Vulnerability Information Table
Technology Reference	Number	Yes	Recommended	Reference to the specific technology in the Technologies Table. This mapping can be made via IP (temporal), hostname, or Reverse DNS depending on implementation details.
Date of Detection	Date/Time	No	Yes	Date and time when the vulnerability was detected
Date of Remediation	Date/Time	No	No	Date and time when the vulnerability was remedied.
Vulnerability Status	Text	No	No	Current Status of the Vulnerability. Uses value *Open* or *Remedied*.
Collateral Damage Potential	Text	No	No	Potential for loss of through damage or theft of the asset. Uses value *None*, *Low*, *Low-Medium*, *Medium-High*, *High*, or *Not Defined*.
Target Distribution	Text	No	No	Proportion of vulnerable systems. Uses value *None*, *Low*, *Medium*, *High*, or *Not Defined*.

Example: Metric Definition

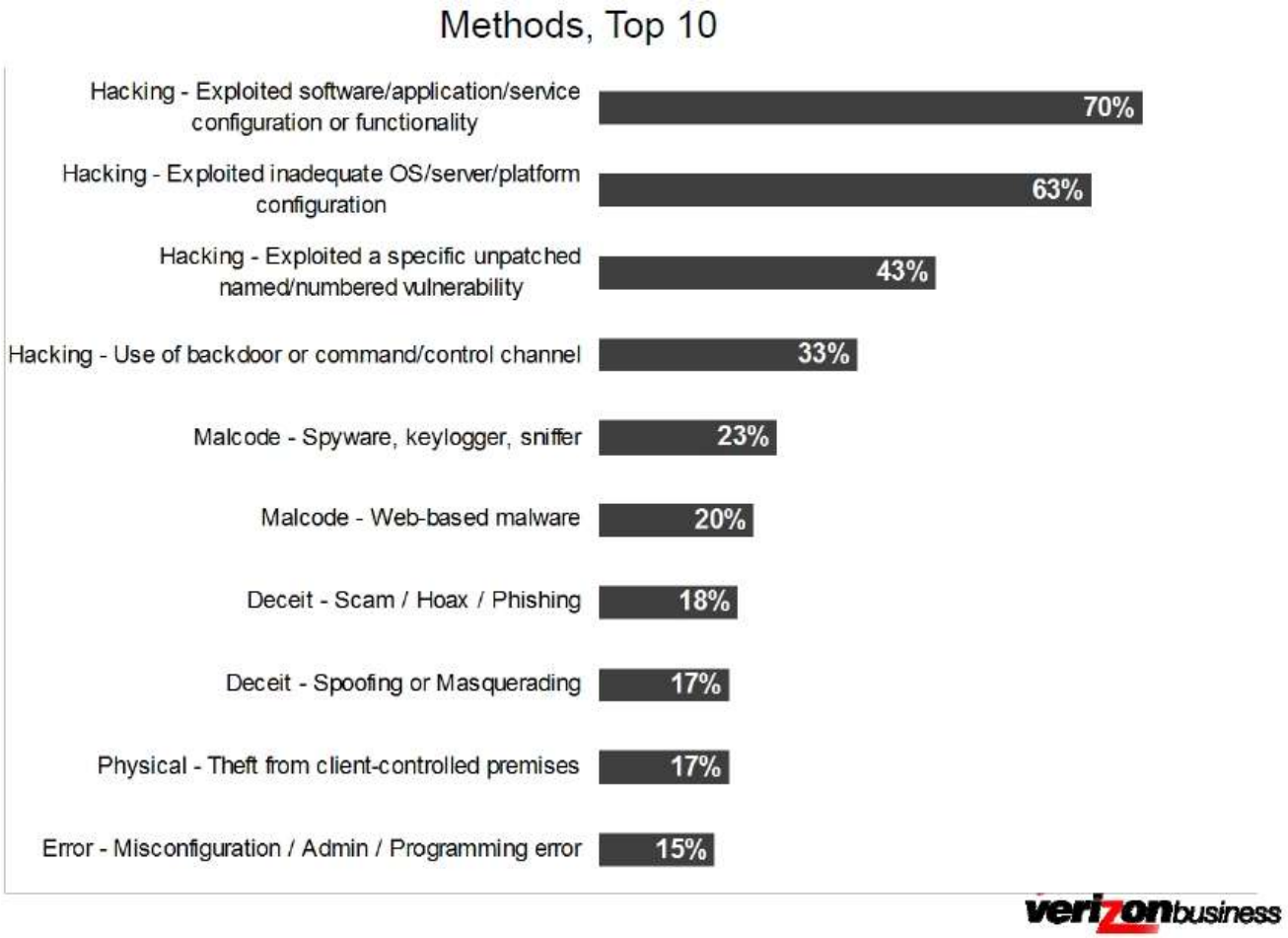
Metric Name	Number of Known Vulnerability Instances
Version	1.0
Status	Draft
Description	Number of Known Vulnerability Instances (NKVI) measures the number of known vulnerability instances as identified during an organization's vulnerability identification process.
Audience	Operations
Question	How many vulnerability instances were found during the time period?
Answer	A positive integer value that is greater than or equal to zero. A value of "0" indicates that no instances of known vulnerabilities were found.
Formula	This metric is calculated by counting the number of vulnerability instances identified. This count should also be done for each severity value (Low, Medium, and High): *Number of Vulnerabilities = Count(Instances of Identified Vulnerabilities)*
Units	Number of Vulnerabilities
Frequency	Weekly, Monthly, Quarterly, Annually
Targets	No consensus values currently exist for this metric. In the ideal case, there would be no known vulnerability instances on any technologies.

Question the metric is asking, and the expected answer format

Description of what the metric is doing

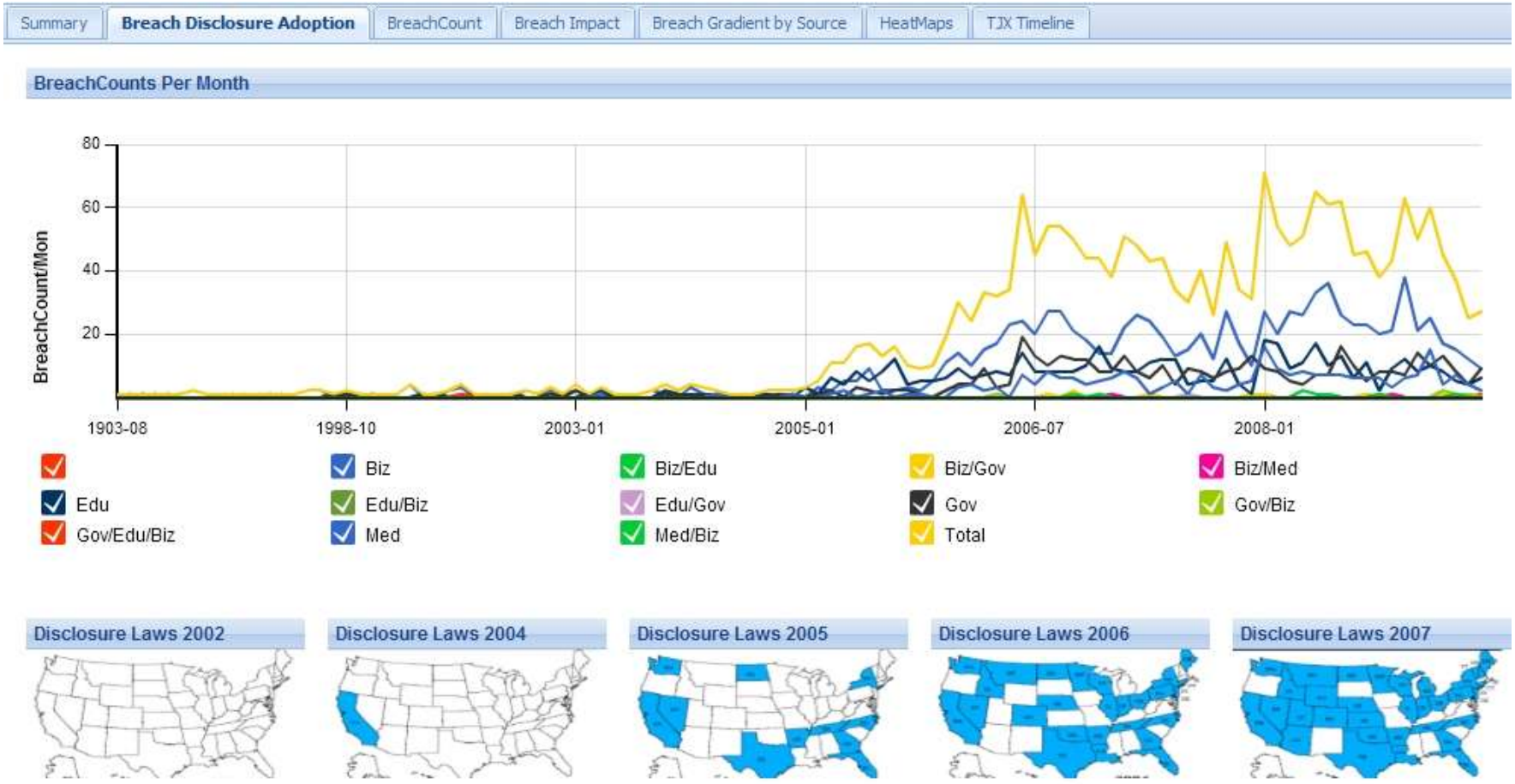
Metric Formula

Example: Insights (Verizon, 2008)



the CENTER for INTERNET SECURITY

Example: Insights (DataLossDB 2008)



the CENTER for INTERNET SECURITY

Next Steps

- Facilitate Adoption and Information Sharing
- Enhance Security Metric Definitions and Coverage
- Publish Quick Start Guide
- Conduct Analysis and Identify High Performers / Best Practice

Call to Action

- **Establish** – business support and goals with senior executives and board of directors
- **Use** – detailed, Consensus Security Metric Definitions and Quick Start Guide from:
  - https://community.cisecurity.org/download
- **Collaborate** – and obtain community help
- **Require** – vendors & consultants to provide and support solutions using community standars

Summary

- Leverage CIS community efforts and experience
- Focus on business outcomes first
- Implement a few metrics that are repeatable
- https://community.cisecurity.org/download
- Contact spiliero@cisecurity.org to participate

the CENTER for INTERNET SECURITY

Questions?

- What are your top 3 security metric requests from leadership?
- What are 3 – 5 application security metrics we can develop?
- What requirements must be addressed for your organization to contribute metrics data to enable performance measurement against peers?

CIS Security Guidance is:

- Available
  - free-of-charge in .pdf format to everyone
  - in tool-readable XML format to CIS Members for use with configuration auditing/monitoring tools
- Used worldwide as
  - the basis for enterprise security standards
  - the recognized standard against which to compare
    - Downloaded >1,000,000 times/year

http//:www.cisecurity.org

spiliero@cisecurity.org
818-425-6129

the CENTER for INTERNET SECURITY