Cybersecurity Metrics History

Jennifer Bayuk

Measures versus Metrics

Measurement is the process of ***mapping*** from the empirical world to the formal, relational world. The measure that results characterizes an ***attribute*** of some object under scrutiny. Information Security is not the object, nor a well-understood attribute.

This means you are not directly measuring security, you are measuring other things and using them to create **Metrics** in order to draw conclusions about security.

Measures versus Numbers

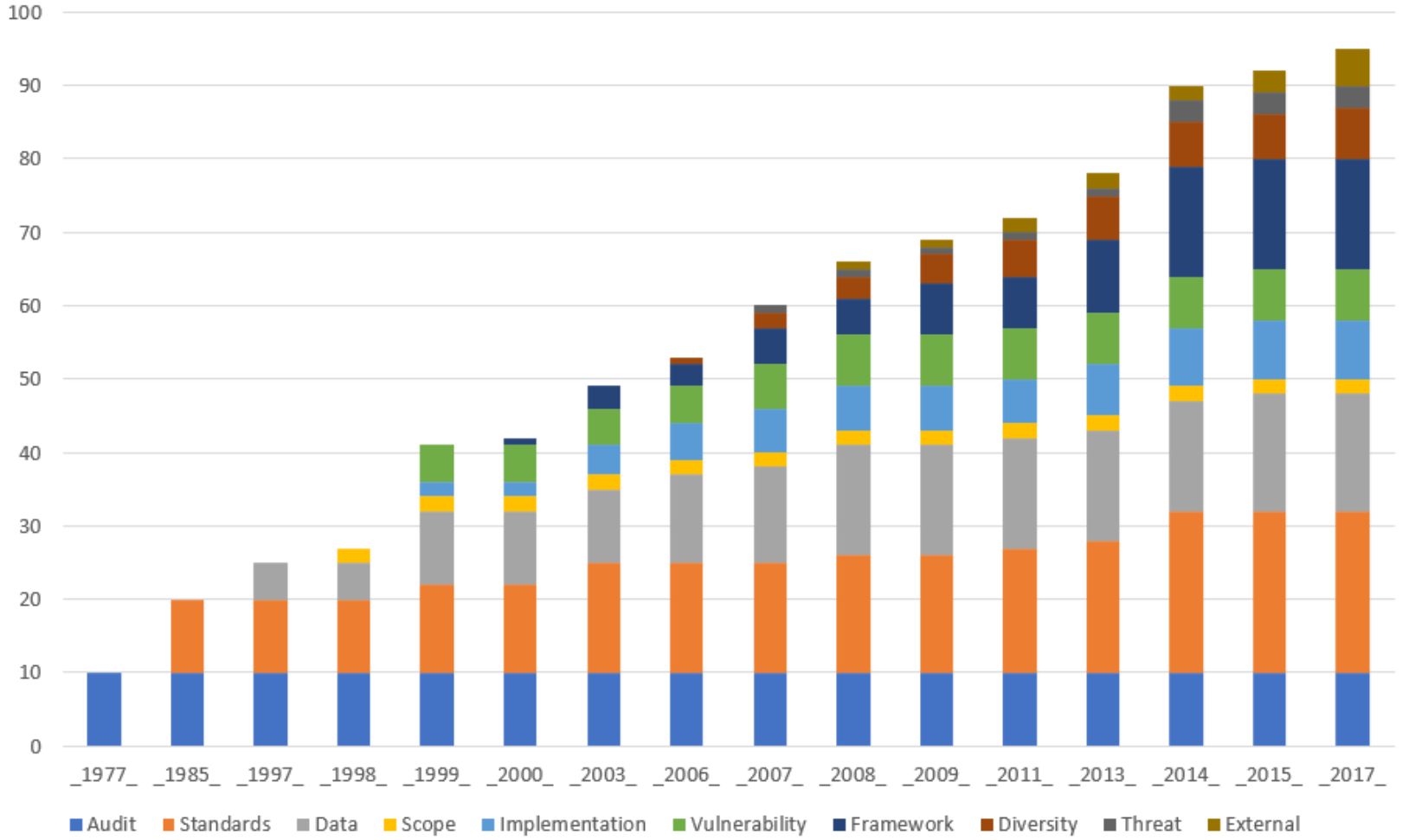
- Nominal – labels (exists, not exists)
- Ordinal – order (low → medium → high)
- Interval – order and quantity (temperature) 
- Ratio – interval with respect to zero (length, dollars) 

See: Herrmann, D. (2007). The Complete Guide to Security and Privacy Metrics. Boca Raton, FL, Auerbach Publications.

Measurement Criteria

Accurate:	data reflects the content of measurement as it was envisioned
Numeric:	data can be precisely quantified
Correct:	data is collected according to specifications
Consistent:	measure is independent of measurer
Time-based:	there is a fixed reference point of data collection
Replicable:	measurement repeated in same manner in same environment will yield same result
Unit-based:	data may be expressed in terms of a unit
Informative:	data provides information without additional context

History of the Practice in Cybersecurity Metrics

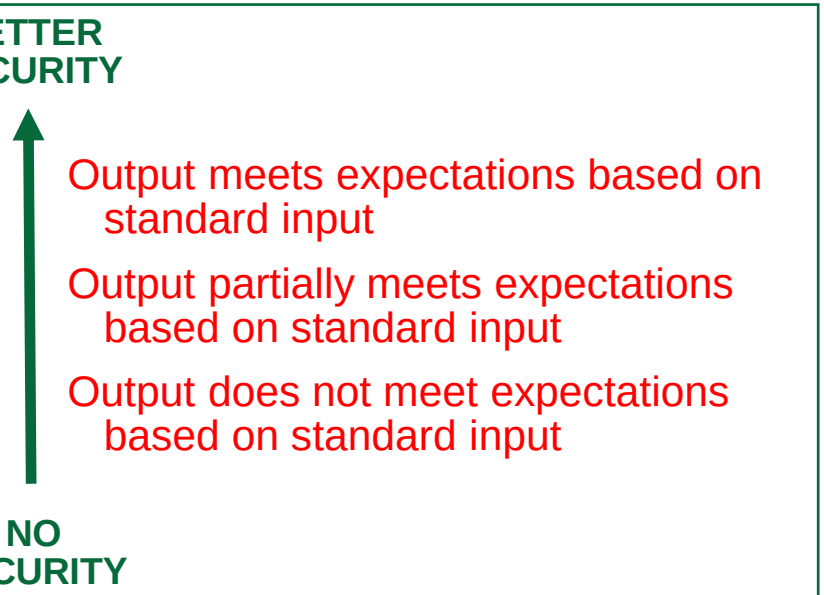


Control Objectives

Standards for management control over computer systems processing published by The Electronic Data Processing Auditors Association, now known as ISACA.

A global consortium was formed to aggregate, review, and agree on technology control:

- Standards
- Procedures
- Guidelines
- Best practices
- Standards for conducting EDP audits entitled "Control Objectives“
- Focused on whether standard input produces expected output



UNITS OF MEASURE → **ATTRIBUTES OF A SINGLE COMPUTER**

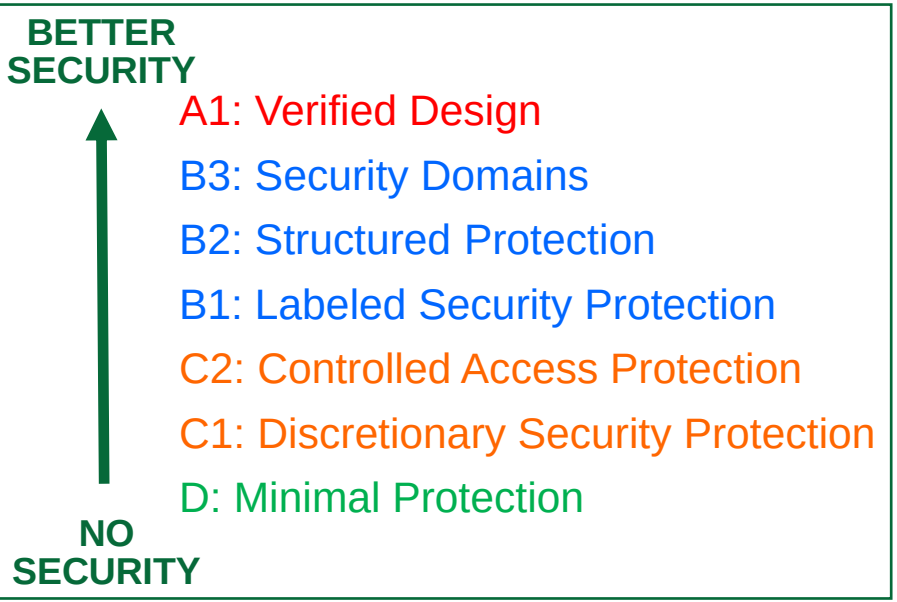
1977

The Orange Book

aka: TCSEC: Trusted Computer System Evaluation Criteria

Standardized Terminology:

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Subjects
- Objects
- Identification
- Authentication
- Audit
- Trusted Path
- Covert Channel



UNITS OF MEASURE → **ATTRIBUTES OF AN OPERATING SYSTEM**

The Orange Book Metric Calculation

From measurable attributes to conclusions about security:

	C1	C2	B1	B2	B3	A1(Verified Design)
Discretionary Access Control	+	+	nc	nc	+	nc
Object Reuse	0	+	nc	nc	nc	nc
Labels	0	0	+	+	nc	nc
Label Integrity	0	0	+	nc	nc	nc
Exporting Labeled Information	0	0	+	nc	nc	nc
Labeling Human-Readable Output	0	0	+	nc	nc	nc
Mandatory Access Control	0	0	+	+	nc	nc
Subject Sensitivity Labels	0	0	0	+	nc	nc
Device Labels	0	0	0	+	nc	nc

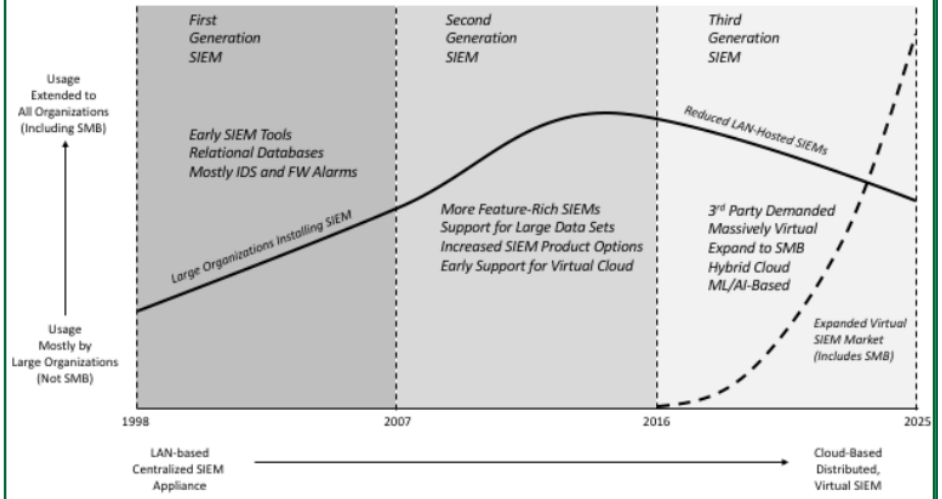
Key: 0: no requirement, +: added requirement, nc: no change

Source: Prof. Ravi Sandhu - profsandhu.com/

Tools for Security Metrics

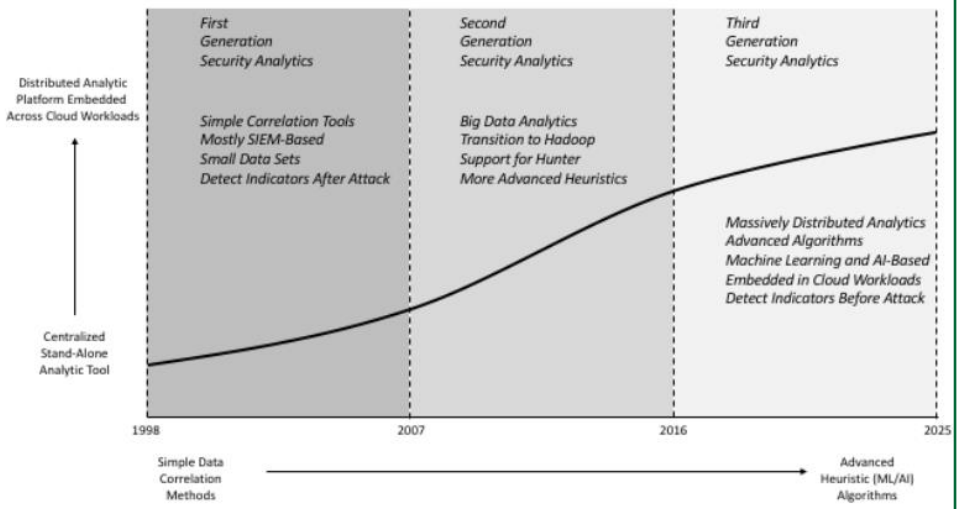
Technology vendors became aware of the appetite for data aggregation in security operations centers and started accommodating with specialized tools.

Security Incident and Event Management



UNITS OF MEASURE: *Incidents, Anomalies*

Security Analytics



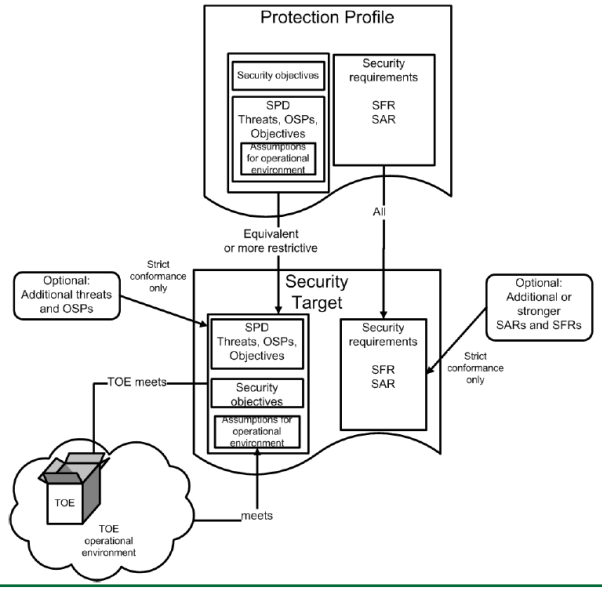
ATTRIBUTES OF *Threats and Vulnerabilities*

Source: TAG Cyber Annual: www.tag-cyber.com

1997

The Common Criteria

A Global consortium acknowledges all systems are different and security must be customized and formally verified.



BETTER SECURITY

NO SECURITY

EAL7: Formally verified, designed and tested
EAL6: Semi-formally verified, designed and tested
EAL5: Semi-formally designed and tested
EAL4: Methodically designed, tested and reviewed
EAL3: Methodically tested and checked
EAL2: Structurally tested
EAL1: Functionally tested

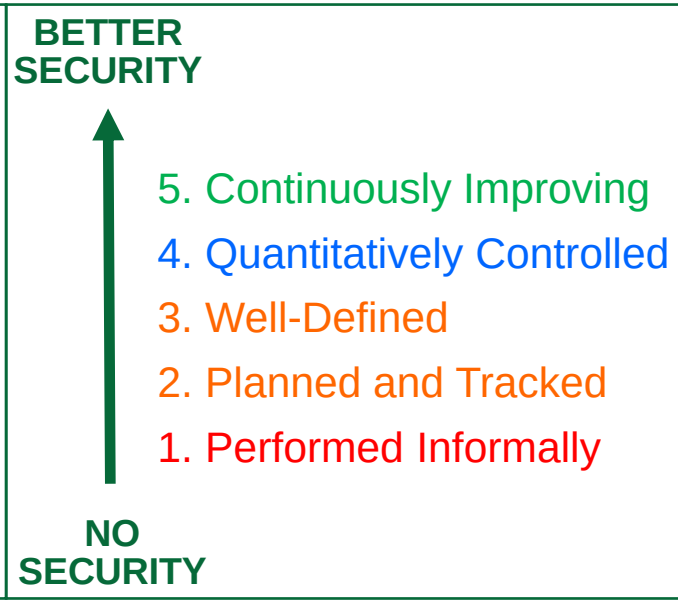
UNITS OF MEASURE → **ATTRIBUTES OF A TARGET OF EVALUATION**

Systems Security Engineering Capability Maturity Model

An influential publication developed by Carnegie Mellon Software Engineering Institute with support from US DoD (*abbreviated as SSE-CMM*).

Specifies security activities to incorporate into the systems engineering lifecycle:

- Administer Security Controls
- Assess Impact
- Assess Security Risk
- Assess Threat
- Assess Vulnerability
- Build Assurance Argument
- Coordinate Security
- Monitor Security Posture
- Provide Security Input
- Specify Security Needs
- Verify and Validate Security



UNITS OF MEASURE → **ATTRIBUTES OF ENGINEERING PROCESS**

National Vulnerability Database

The NVD is a U.S. government repository of security vulnerability management data represented using the Security Content Automation Protocol (SCAP).

This data enables automation of software vulnerability identification via publication of:

- unique vulnerability identifier
- security checklist references
- security-related software flaws
- security-related misconfigurations
- baseline vulnerability impact metrics

BETTER SECURITY

NO SECURITY

The NVD includes a Common Vulnerability Scoring System (CVSS) Calculator to help evaluate risk of negative impact from any given vulnerability.

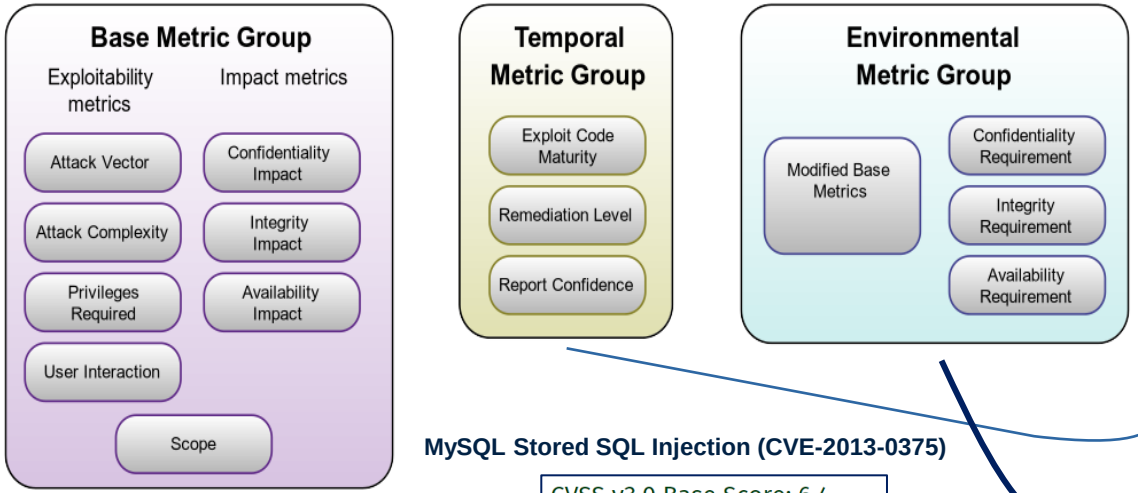
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

UNITS OF MEASURE → **ATTRIBUTE OF SOFTWARE VULNERABILITY**

1999

Common Vulnerability Scoring System (CVSS)

Indirectly analyzes threat by assessing how easy it is to exploit a vulnerability. Initial score is set by the Forum of Incident Response and Security Teams (FIRST), and organizations may customize.



Acronym	Measure	Possible Values
MAV	Modified Attack Vector	[X,N,A,L,P]
MAC	Modified Attack Complexity	[X,L,H]
MPR	Modified Privileges Required	[X,N,L,H]
MUI	Modified User Interaction	[X,N,R]
MS	Modified Scope	[X,U,C]
MC	Modified Confidentiality	[X,N,L,H]
MI	Modified Integrity	[X,N,L,H]
MA	Modified Availability	[X,N,L,H]
E	Exploit Code Maturity	[X,H,F,P,U]
RL	Remediation Level	[X,U,W,T,O]
RC	Report Confidence	[X,C,R,U]
CR	Confidentiality Req.	[X,H,M,L]
IR	Integrity Req.	[X,H,M,L]
AR	Availability Req.	[X,H,M,L]

MySQL Stored SQL Injection (CVE-2013-0375)

CVSS v3.0 Base Score: 6.4

Metric	Value	Metric	Value
Attack Vector	Network	Confidentiality Impact	Low
Attack Complexity	Low		
Privileges Required	Low	Integrity Impact	Low
User Interaction	None	Availability Impact	None
Scope	Changed		

Example Values:

A = Adjacent
C = Critical
F - Functional exploit code exists
H = High
L = Local
M = Medium
N = None, No impact, Network
O = Official Fix Available
P = Proof of concept exploit code exists
R = Reasonable
T = Temporary Fix Available
U = Unknown, Unavailable, Unproven
W = Workaround Available
X = Not Applicable

https://nvd.nist.gov/vuln-metrics/cvss

National Institute of Standard and Technology

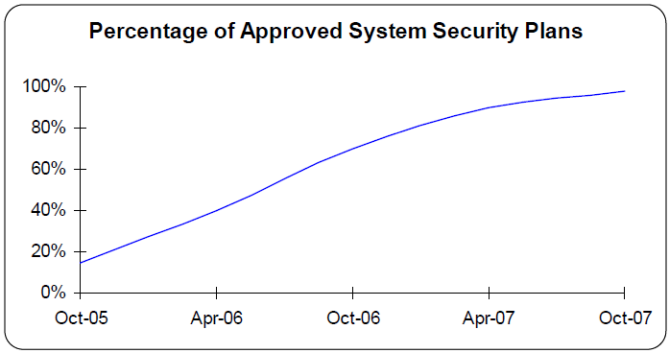
Performance Measurement Guide for Information Security (Special Publication 800-55 Rev 1, first version 2003).

Fundamentally a Goal, Question Metric Approach where the goals are *implementation*, *effectiveness*, *efficiency*, and *impact* for each critical element of the security program, as defined in self-assessment requirements.*

BETTER SECURITY

NO SECURITY

800-55 specifies that each security program critical element should have trending metrics and provides examples such as:



UNITS OF MEASURE → **ATTRIBUTES OF A SECURITY PROGRAM**

*In 2003, the goals came from SP800-26, *Security, Self-Assessment Guide for Information Technology Systems*. A 2008 Revision changed this citation to SP800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*.

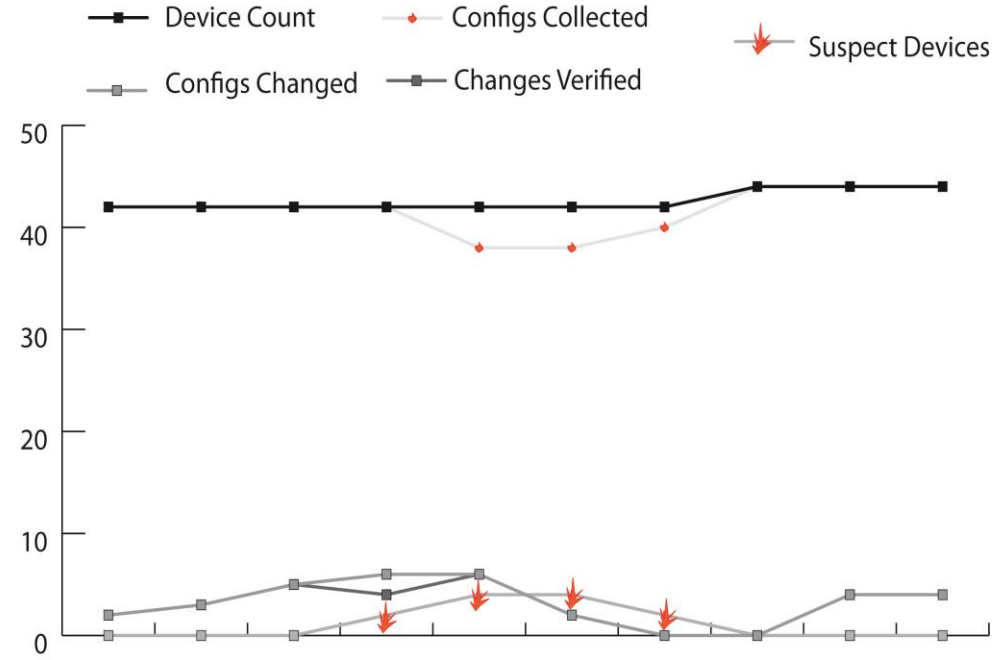
Example Enterprise Adoption of SP800-55

Measure W:
The number of firewall devices in operation.

Measure X:
The number of firewall devices whose configuration was retrieved in past 24 hours by network management system.

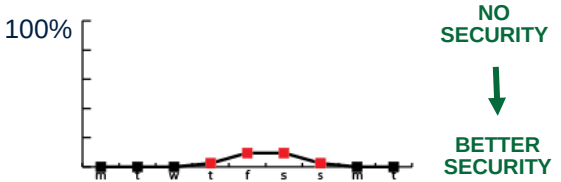
Measure Y:
The number of firewall devices configurations that deviate from yesterday's configuration.

Measure Z:
The number of deviant device configurations where deviations directly compare to authorized planned changes.



UNITS OF MEASURE → **ATTRIBUTES OF A SECURITY PROGRAM**

Network Periphery Control Performance Metric:
Suspect Devices as % of Total: ((W-X) + (Y-Z)) / W



Metricon

A periodic meeting of specialists in cybersecurity metrics was formed by Dan Geer and Andy Jaquith, and drew dozens of volunteer program committee participants as well as sponsors.

Presentations cover a variety of cybersecurity metrics categories, including but not limited to:

Adversary Skills:	Metrics that estimate adversary skills levels.
Adversary Goals:	Metrics gleaned from intelligence on adversary motivation and justification.
Deterministic Models:	Metrics that combine measures with inference rules (e.g. artificial intelligence) to form conclusions about cybersecurity.
External activity:	Metrics that track threats (“weather”).
Internal activity:	Metrics that chart work activity (“busyness”).
Performance:	Metrics that demonstrate capability to deliver system features.
Process Monitor:	Metrics that monitor security processes.
Remediation:	Metrics that show progress toward a security objective.
Resilience:	Metrics that demonstrate system ability to recover from harmful impact.
Stochastic Models:	Metrics that combine measures with probability estimates based on historical data.
Target:	Metrics that have a measurable 100% target.
Vulnerability:	Metrics that show susceptibility to known threats.

As consensus matured, Metricon attendees published several textbooks, including but not limited to:

- Jennifer Bayuk: Stepping Through the InfoSec Program
- Fred Cohen: IT Security Governance Guidebook with Security Program Metrics on CD-ROM (The CISO Toolkit 1)
- Lance Hayden: IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data
- Jay Jacobs and Bob Rudis: Data-Driven Security: Analysis, Visualization and Dashboards
- Andrew Jaquith: Security Metrics: Replacing Fear, Uncertainty, and Doubt
- Richard Seiersen: The Metrics Manifesto: Confronting Security with Data
- Caroline Wong: Security Metrics, A Beginner's Guide

Validation Metric: Threat Intelligence

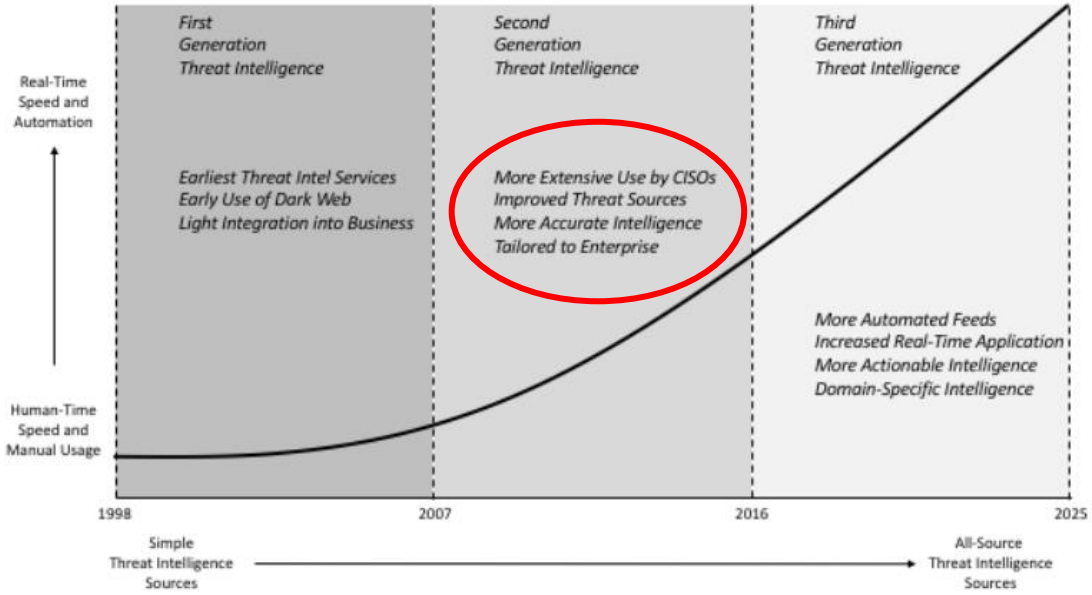
Cybersecurity vendors customize threat hunting to find evidence of a company's data breach on the dark web.

Customized metrics on:

Internal Data found on dark web
Mail sent from lookalike Domains
Lookalike Websites

Delivered in bulk via:

- TAXII™, the Trusted Automated eXchange of Indicator Information;
- STIX™, the Structured Threat Information eXpression; and
- CybOX™, the Cyber Observable eXpression.



UNITS OF MEASURE: → **ATTRIBUTES OF** *Targeted (maybe successful) Attacks*

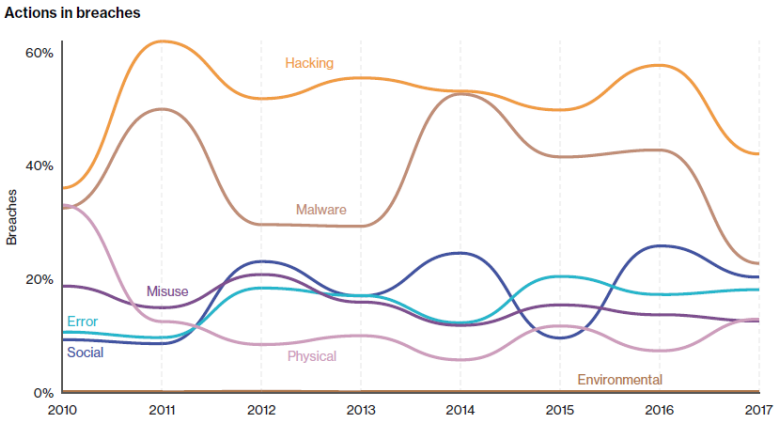
Source: TAG Cyber Annual: www.tag-cyber.com

2007

Verizon Data Breach Incident Report

An annual analysis of data breach incidents collected by dozens of cybersecurity service providers and law enforcement agencies world-wide.

		Incidents									Breaches								
		Accommodation (72)	Education (61)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Professional (54)	Public (92)	Retail (44-45)	Accommodation (72)	Education (61)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Professional (54)	Public (92)	Retail (44-45)
Pattern	Crimeware	17	31	52	76	206	58	60	4,758	21	3	3	7	1	3	5	8	8	3
	Web Applications	14	30	76	71	75	40	79	93	92	14	24	70	65	45	36	73	33	88
	Privilege Misuse	1	19	100	110	14	36	13	13,021	16	1	9	45	85	7	14	10	40	14
	Everything Else	7	24	29	39	23	23	59	61	14	3	20	12	27	17	8	26	37	8
	Denial of Service		226	575	3	684	163	408	992	54							1		
	Cyber-Espionage	1	6	32	3	22	16	9	143	2	1	5	22	2	20	13	8	140	2
	Miscellaneous Errors	5	37	36	104	69	14	30	1,515	12	2	35	34	97	65	12	28	58	11
	Lost and Stolen Assets	4	9	9	62	4	5	14	2,820	7	1	3	2	28	1	2	5	16	3
	Point of Sale	40			2					10	38			2					9
	Payment Card Skimmers			21		1				10			18		1				4
Action	Malware	61	50	96	85	244	88	91	4,922	90	46	16	33	7	33	26	29	153	70
	Hacking	45	279	699	100	796	233	524	1,279	162	42	42	95	78	75	58	100	205	102
	Misuse	1	19	100	110	14	36	13	13,021	16	1	9	45	85	7	14	10	40	14
	Social	18	43	88	91	38	56	100	201	15	14	38	69	78	32	42	69	173	10
	Error	5	40	38	124	72	16	37	4,317	15	2	37	36	110	67	13	31	66	14
	Physical	5	6	32	47	5	4	8	20	16	2	1	18	17	2	2	3	9	6



BETTER SECURITY

No overlap in your data and report

Data from your peers in report

Your data in report

NO SECURITY

UNITS OF MEASURE → **ATTRIBUTES OF A CYBERATTACK**

2008

Directions in Security Metrics Research (NISTIR7564)

The report followed SP-55-Rev1 and emphasized the difference between

Correct

security performance an

Effective

security performance.

This is the same distinction made by SSE-CMM as:

Verification

versus

Validation

Security

In systems engineering terms:

Building the system right

versus

Building the right system

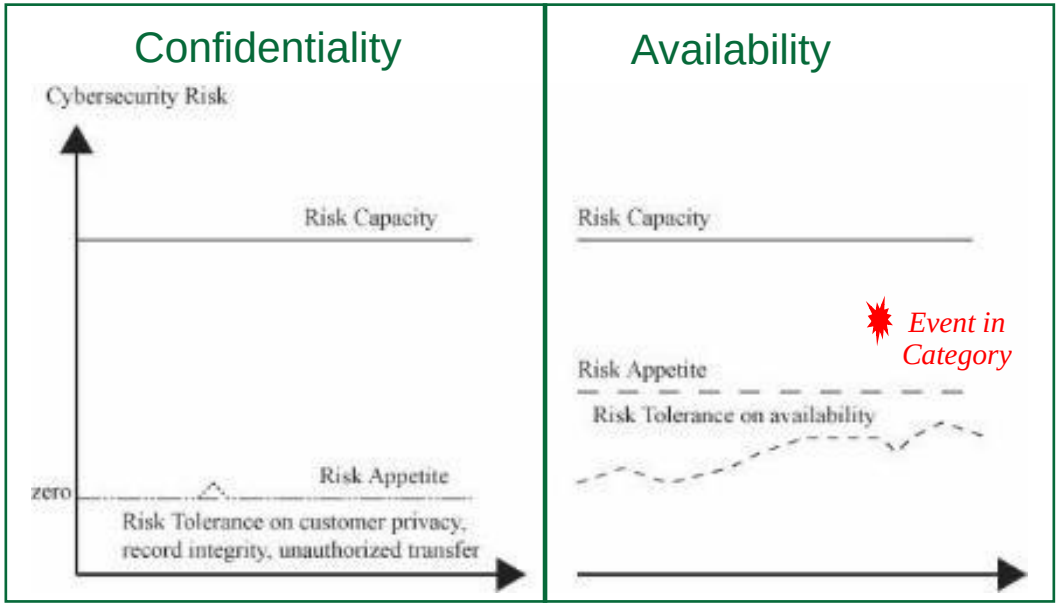
"The current practice of security assessment, best illustrated by lower level evaluations under the Common Criteria, emphasizes the soundness of the evaluation evidence of the design and the process used in developing a product over the soundness of the product implementation. The rationale is that without a correct and effective design and development process, a correct and effective implementation is not possible. While this is true, the

*emphasis on **design and process evidence** versus **actual product software** largely overshadows practical security concerns involving the implementation and deployment of operational systems."*

– Note - NISTIR 7564 author (Wayne Jansen) was at this time an active Metricon program committee member

Cybersecurity Viewed as Operational Risk

- For each cybersecurity risk (e.g. confidentiality, availability), qualitatively declare Risk Appetite far lower than Risk Capacity
- Qualitative Risk Appetite is be measured with quantifiable Risk Tolerance Metrics
- Investigate negative trends in tolerance metrics to determine whether:
  - Tolerance metrics sound justified alarms; or
  - Tolerance metrics need to be revised and recomputed



Note: though trends are intended to be correlated with probability, actual negatively impacting events may result in breach of appetite and/or a reexamination of tolerance measures

UNITS OF MEASURE → **ENTERPRISE RISK TOLERANCE**

2013

NIST Cybersecurity Framework

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Metric NIST-CSF: Coverage of NIST-CSF

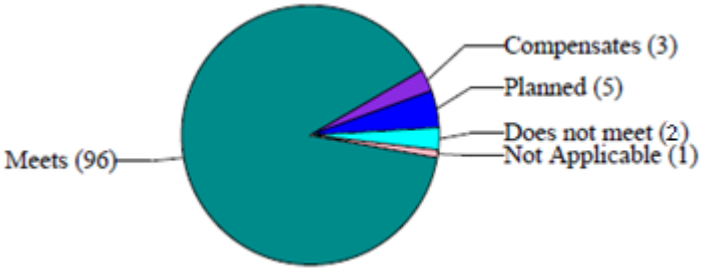
Category:	Performance
Description:	Report of gaps in coverage of NIST CSF functions with existing security controls and tools.
Scope:	Cybersecurity Program
Measure:	NIST-Controls - Controls Map to NIST, (Subcategory,Control)
Measure:	NIST-Target - NIST CSF , Subcategory
Measure:	NIST-Tools - Tools Map to NIST, (Subcategory,Tool)
Algorithm:	For each SUBCATEGORY in NIST-TARGET: If SUBCATEGORY not in NIST-Controls or NIST-Tools Potential_Gap.append(SUBCATEGORY) For SUBCATEGORY in Potential_Gap: List SUBCATEGORY
Unit:	Subcategory
Interval:	Monthly
Basis for KRI:	Cybersecurity Standards
Explanation:	Coverage of NIST-CSF with Security Policies, Controls, and Tools
Comparison:	Equals Threshold
Threshold:	Target Profile
Use Case:	Leading

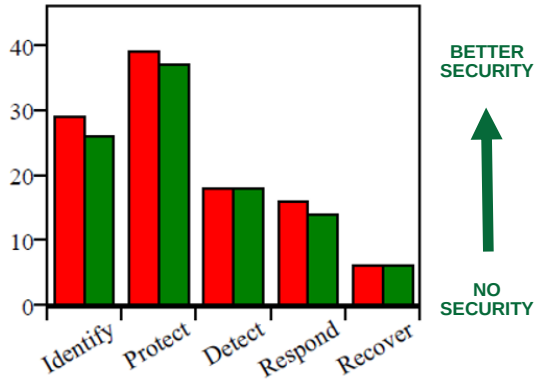
UNITS OF MEASURE: Subcategories → **ADEQUACY OF A SECURITY PROGRAM**

2014

Source: https://www.nist.gov/cyberframework, updated 2018

Enterprise Example: SP800-55 NIST-CSF Coverage for SP800-53





Enterprises are encouraged to set their own targets at a subcategory level.

Section Status:

IDENTIFY: 100% complete, 2 compensated, 1 planned, 2 not met, section has 78 control links and 1 evidence attachments section has 2 flagged issues

PROTECT: 100% complete, 2 compensated, 3 planned, 1 not applicable, section has 233 control links and 0 evidence attachments section has 3 flagged issues

DETECT: 100% complete, 1 planned, section has 125 control links and 7 evidence attachments section has 1 flagged issues

RESPOND: 100% complete, section has 72 control links and 2 evidence attachments section has 0 flagged issues

RECOVER: 100% complete, section has 18 control links and 0 evidence attachments section has 0 flagged issues

Total number of Requirements: 108

Count Completed: 108

Total so far fully met: 96, 88.9%

Total number of Requirements with linked controls: 102

Total number of Requirements with linked evidence: 10

GAPS

ID.AM-3: Organizational communication and data flows are mapped, Response: Compensating Control

ID.RM-2: Organizational risk tolerance is determined and clearly expressed, Response: Plans to Meet

ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process, Response: Compensating Control

ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations., Response: Does not Meet

ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers, Response: Does not Meet

Framework Metrics produced by FrameCyber, see www.framecyber.com

Security Scorecard Standards

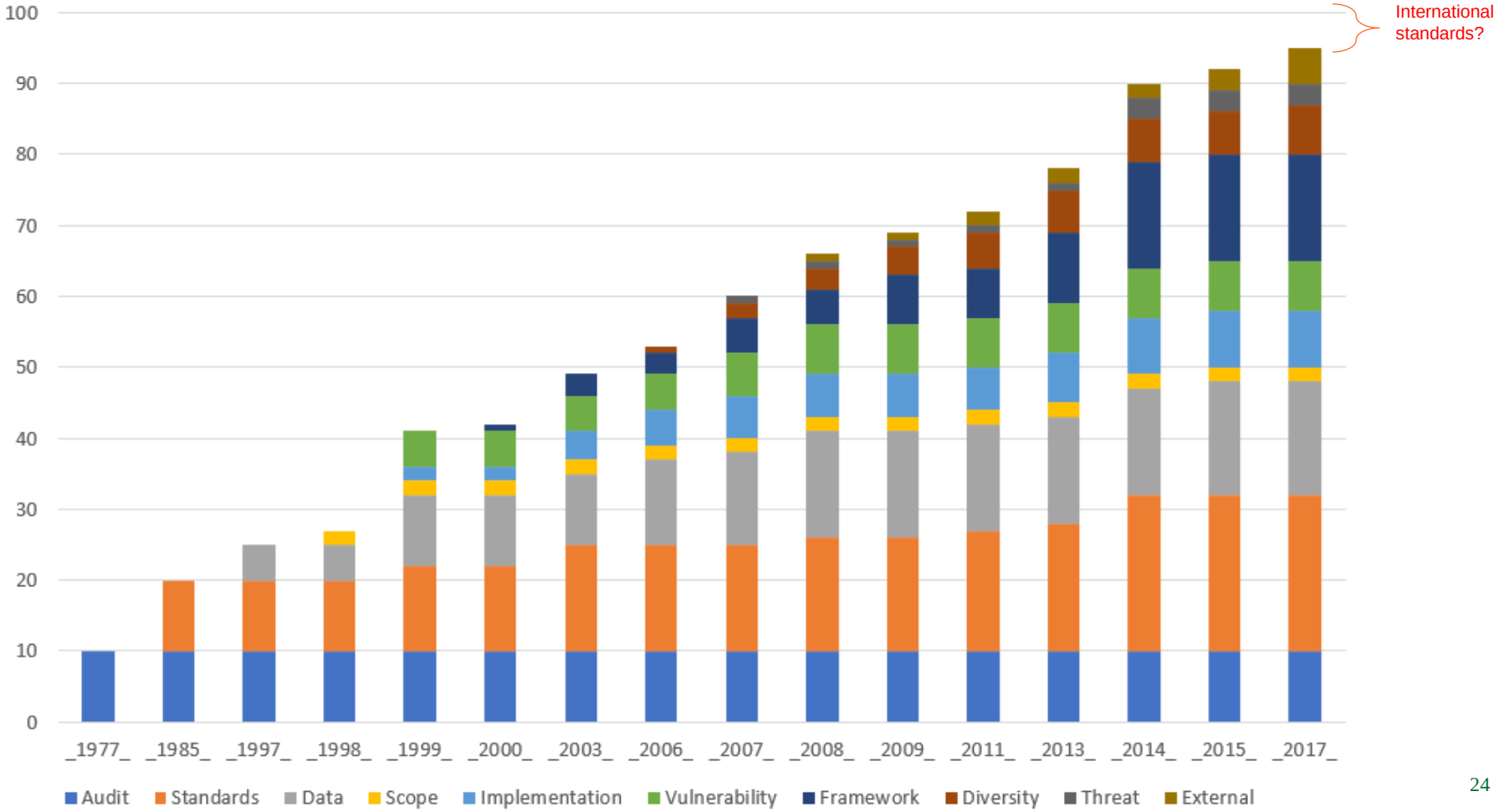
Transparency:	Rating companies shall provide sufficient transparency into the methodologies and types of data used to determine their ratings, including information on data origination as requested and when feasible, for customers and rated organizations to understand how ratings are derived. Any rated organization shall be allowed access to their individual rating and the data that impacts a change in their rating.
Dispute, Correction and Appeal:	Rated organizations shall have the right to challenge their rating and provide corrected or clarifying data. Rating companies should have an appeal and dispute resolution process. Disputed ratings should be notated as such until resolved.
Accuracy and Validation:	Ratings should be empirical, data-driven, or notated as expert opinion. Rating companies should provide validation of their rating methodologies and historical performance of their models. Ratings shall promptly reflect the inclusion of corrected information upon validation.
Model Governance:	Prior to making changes to their methodologies and/or data sets, rating companies shall provide reasonable notice to their customers and clearly communicate how announced changes may impact existing ratings.
Independence:	Commercial agreements, or the lack thereof, with rating companies shall not have direct impact on an organization's rating; any rated organization will be able to see and challenge their rating irrespective of whether they are a customer of the rating company.
Confidentiality:	Information disclosed by a rated organization during the course of a challenged rating or dispute shall be appropriately protected. Rating companies should not publicize an individual organization's rating. Rating companies shall not provide third parties with sensitive or confidential information on rated organizations that could lead directly to system compromise.

UNITS OF MEASURE: ????? → **SPECTATOR OPINION OF FIRM SECURITY**

2017

Source: https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings

State of the Practice in Security Metrics



Thank you!

https://www.framecyber.com
Publications available at: https://www.bayuk.com

jen@framecyber.com
jennifer@bayuk.com