Cyber Security Metrics

Mischel Kwon
MKA

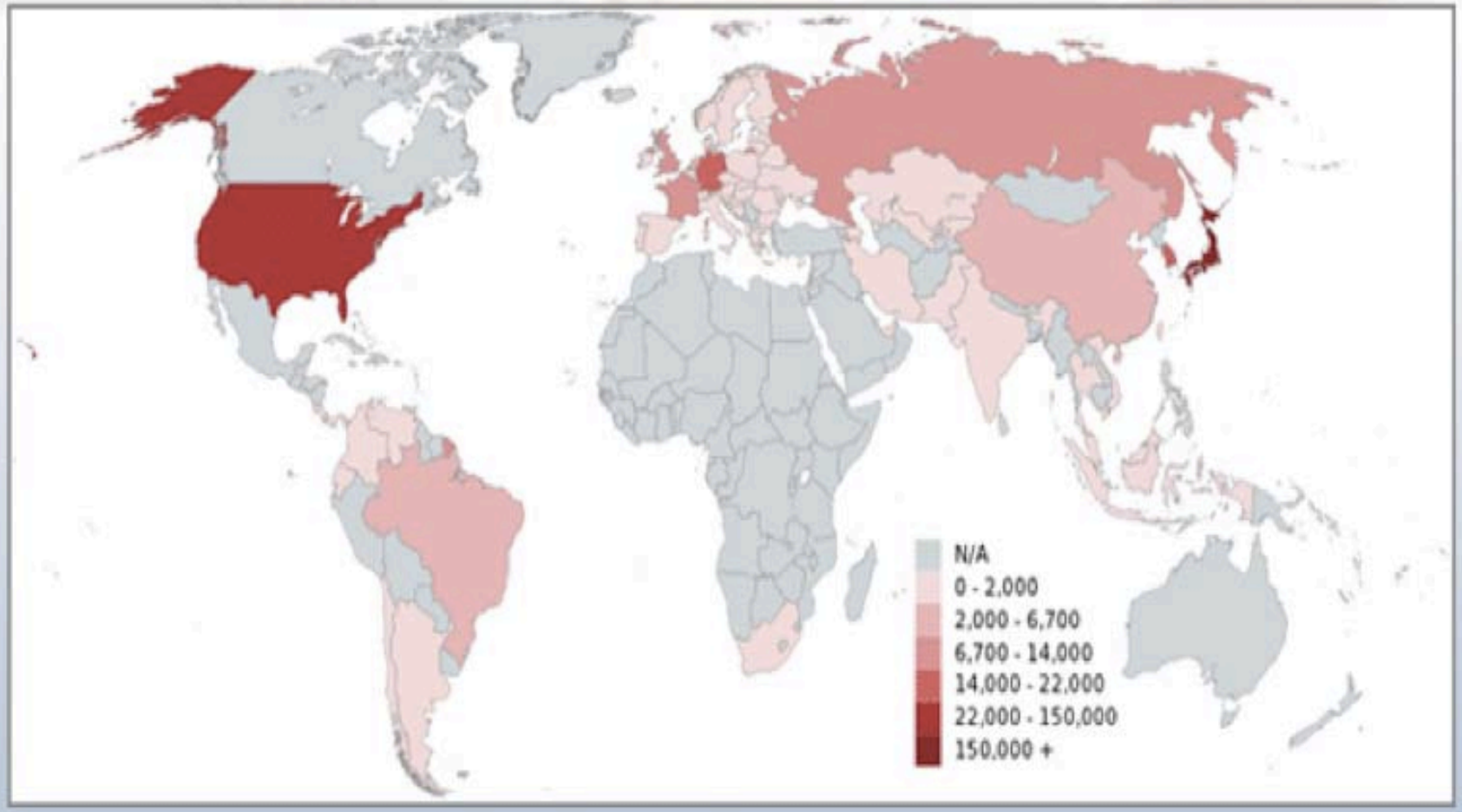
2/27/2012

MiniMetricon 6.5

Cyber Metrics Today

- Metrics (actionable) or Statistics (interesting)?
- Clear purpose for metrics – today it's scrabbled eggs
  - Capability
  - Reduction of attacks
  - Reduction of individual actions
  - Compliance
- Begins with taxonomy – still chasing the pieces and parts
- Real failure – the data – the collection – very subjective
- No Actionable Results
  - Understanding the scope of an incident
  - What is the ultimate goal of the incident
  - Less to do with individual events – everything to do with patterns

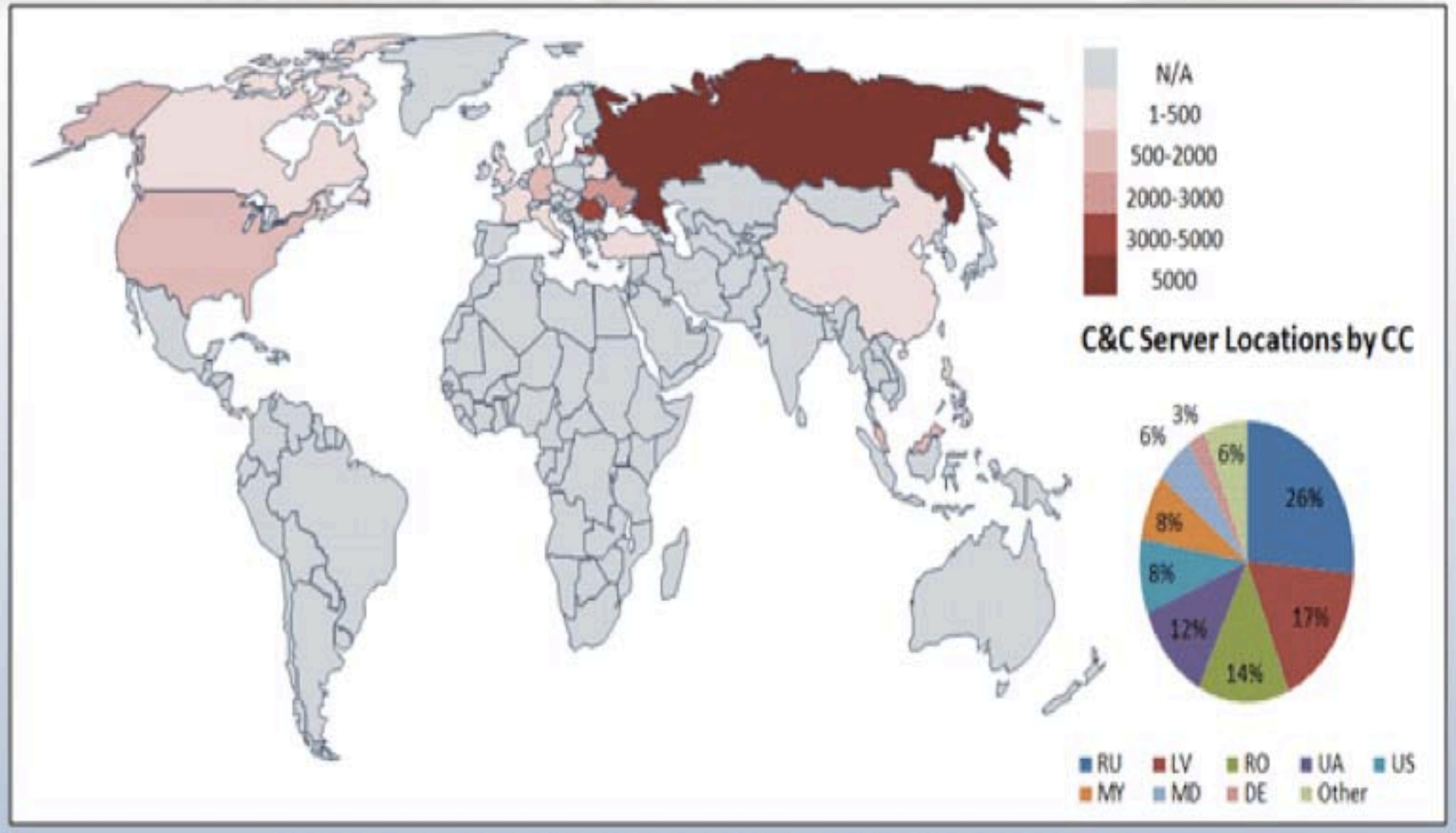
Threats Spreading Geographically



Geographic distribution of global hosted threats observed in December 2011 (iSIGHT Partners)

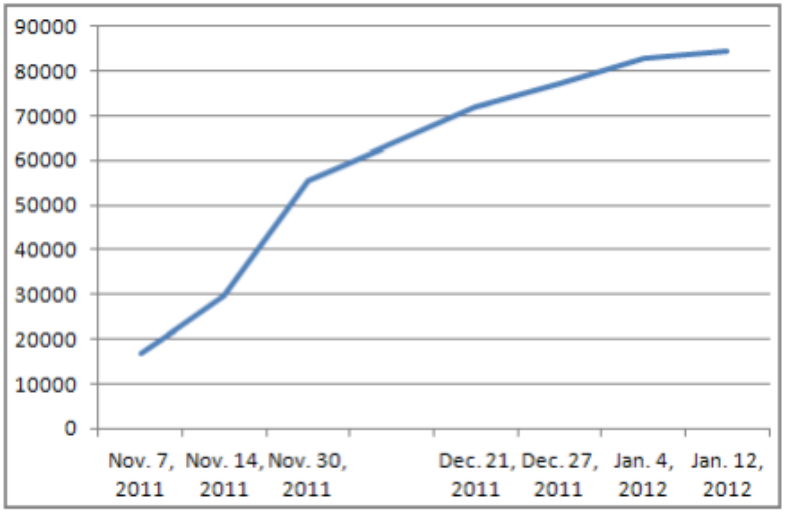
iSIGHTPARTNERS

Threats Spreading Geographically

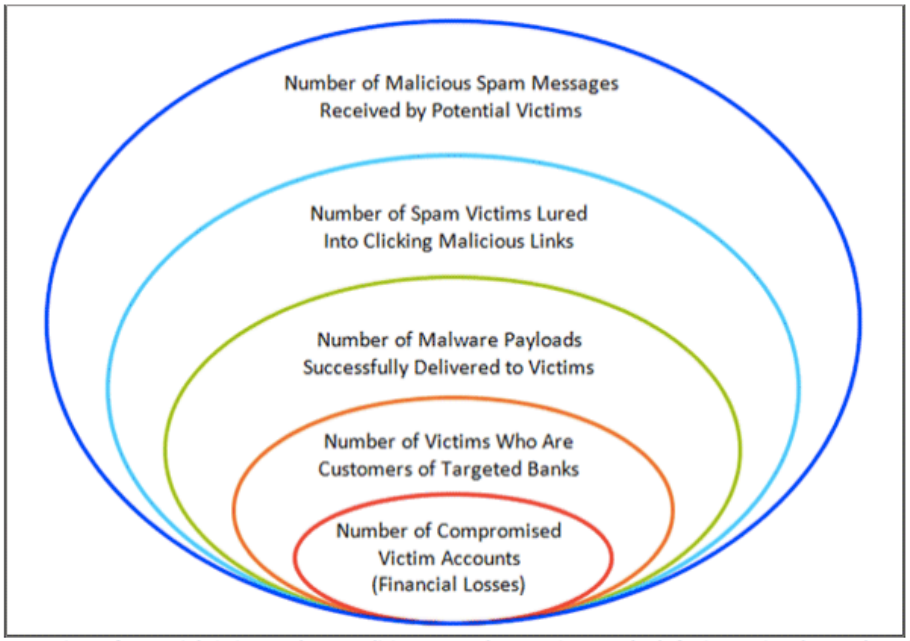


Botnet C&C servers and their geographic distribution (iSIGHT Partners)

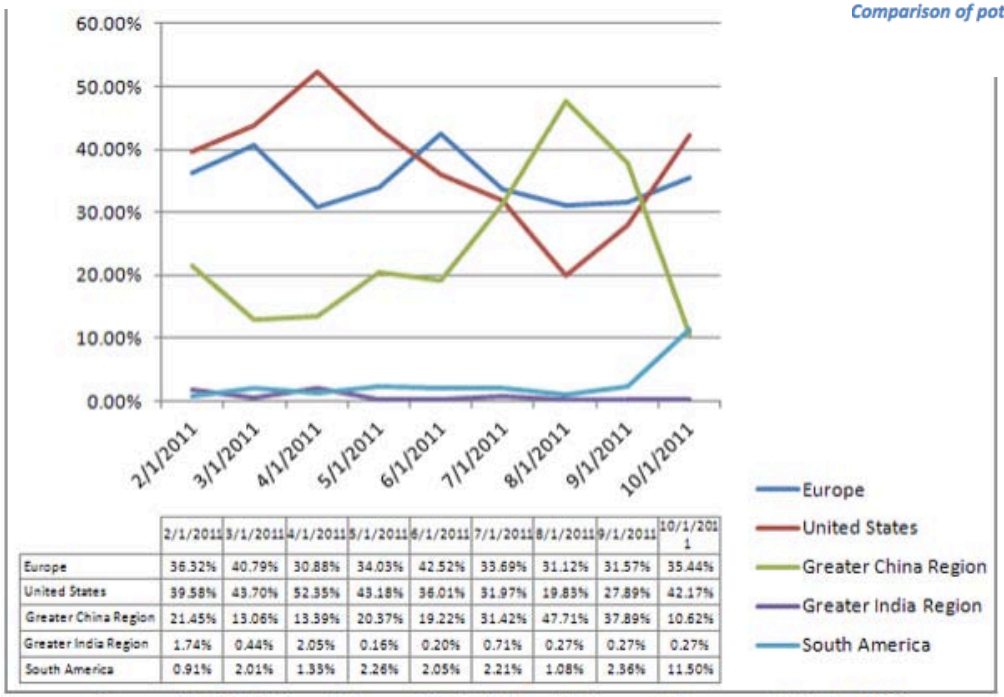
iSIGHTPARTNERS
Security beyond the edge



Number of Gameover Zeus drones over time, demonstrating a slowing growth rate (iSIGHT Partners)



Comparison of potential victim numbers. Malicious actors have various methods for increasing the number of potential victims at multiple stages of an eCrime operation (iSIGHT Partners)



	2/1/2011	3/1/2011	4/1/2011	5/1/2011	6/1/2011	7/1/2011	8/1/2011	9/1/2011	10/1/2011
Europe	36.32%	40.79%	30.88%	34.03%	42.52%	33.69%	31.12%	31.57%	35.44%
United States	39.58%	43.70%	52.35%	43.18%	36.01%	31.97%	19.83%	27.89%	42.17%
Greater China Region	21.45%	13.06%	13.39%	20.37%	19.22%	31.42%	47.71%	37.89%	10.62%
Greater India Region	1.74%	0.44%	2.05%	0.16%	0.20%	0.71%	0.27%	0.27%	0.27%
South America	0.91%	2.01%	1.33%	2.26%	2.05%	2.21%	1.08%	2.36%	11.50%

Geographic distribution of observed hosted threats between February and October 2011 (iSIGHT Partners)

Approximately 400,000 to 500,000 hosted threats on average were observed each month from February to October 2011. The top three regions in terms of hosted threats were the United States, Europe and the Greater China Region

For most of this period, the US led with the highest number of hosted threats, seeing increased observed incidents throughout the first quarter of 2011.

NIST 800-61

US-CERT Quarterly Trend Report

Category	Name	Description
CAT 1	Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.
CAT 2	Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
CAT 3	Malicious Code	*Successful* installation of malicious software (e.g., virus, worm, spyware, bots, Trojan horse, or other code-based malicious entity that infects or affects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.
CAT 4	Improper Usage	A person violates acceptable computing use policies
CAT 5	Scans, Probes, or Attempted Access	Any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
CAT 6	Investigation	*Unconfirmed* incidents of potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

01-Unauthorized Access	1.7%
02-Denial of Service	0.2%
03-Malicious Code	4.3%
04-Improper Usage	1.9%
05-Scans/Probes/Attempted Access	88.9%
06-Investigation	3.1%
Total:	100.0%

Federal Government	14.0%
Other	86.0%
Total:	100.0%

NIST Special Pub 800-61

Table 3-3. Excerpt of a Sample Diagnosis Matrix

Symptom	Denial of Service	Malicious Code	Unauthorized Access	Inappropriate Usage
Files, critical, access attempts	Low	Medium	High	Low
Files, inappropriate content	Low	Medium	Low	High
Host crashes	Medium	Medium	Medium	Low
Port scans, incoming, unusual	High	Low	Medium	Low
Port scans, outgoing, unusual	Low	High	Medium	Low
Utilization, bandwidth, high	High	Medium	Low	Medium
Utilization, email, high	Medium	High	Medium	Medium

Table 3-4. Effect Rating Definitions

Value	Rating	Definition
0.00	None	No effect on a single agency, multiple agencies, or critical infrastructure
0.10	Minimal	Negligible effect on a single agency
0.25	Low	Moderate effect on a single agency
0.50	Medium	Severe effect on a single agency or negligible effect on multiple agencies or critical infrastructure
0.75	High	Moderate effect on multiple agencies or critical infrastructure
1.00	Critical	Severe effect on multiple agencies or critical infrastructure

Table 3-5. Criticality Rating Definitions

Value	Rating	Definition
0.10	Minimal	Non-critical system (e.g., employee workstations), systems, or infrastructure
0.25	Low	System or systems that support a single agency's mission (e.g., DNS servers, domain controllers), but are not mission critical
0.50	Medium	System or systems that are mission critical (e.g., payroll system) to a single agency
0.75	High	System or systems that support multiple agencies or sectors of the critical infrastructure (e.g., root DNS servers)
1.00	Critical	System or systems that are mission critical to multiple agencies or critical infrastructure

NIST Special Pub 800-61 continued

To determine the overall severity rating for an incident, organizations should use the following formula:

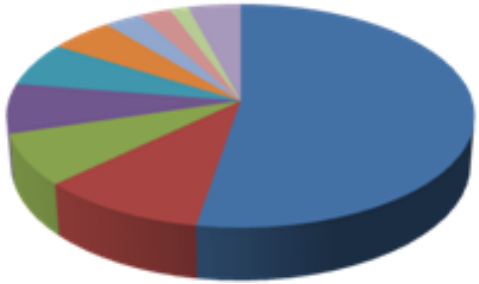
Overall Severity/Effect Score = Round ((Current Effect Rating * 2.5) + (Projected Effect Rating * 2.5) + (System Criticality Rating * 5))

Using the resulting score, organizations can apply the respective overall rating to the incident, as shown in Table 3-6.

Table 3-6. Incident Impact Rating

Score	Rating
00.00 – 00.99	None
01.00 – 02.49	Minimal
02.50 – 03.74	Low
03.75 – 04.99	Medium
05.00 – 07.49	High
07.50 – 10.00	Critical

FISMA FY10



Phishing	56,579	52.7%
Virus/Trojan/Worm/Logic Bomb	11,001	10.2%
Malicious Web Site	7,971	7.4%
Non Cyber	7,741	7.2%
Policy Violation	6,888	6.4%
Equipment Theft/Loss	5,395	5.0%
Suspicious Network Activity	3,121	2.9%
Attempted Access	2,712	2.5%
Social Engineering	1,571	1.5%
Others	4,460	4.2%
Total	107,439	100.0%

Source: US-CERT

Table 1. Incidents Reported to US-CERT by Federal Agencies in FY 2010

Incidents Category	# of Incidents	% of Total Incidents
Unauthorized Access	5,775	13.8%
Denial of Service	23	0.1%
Malicious Code	12,864	30.8%
Improper Usage	7,329	17.5%
Scans, Probes, and Attempted Access	4,419	10.6%
Under Investigation / Other	11,336	27.2%
Total	41,776	100.0%

Data, Collection Method, Analysis

- Subjective
- Reporting by phone or form
- Spreadsheets, adhoc reports
- Report de jour – not purpose
- Not even statistics
- Tells us nothing

CIS Metrics

Broad Scope - incident, vulnerability, patch, application, CM, financial

Function	Management Perspective	Defined Metrics
Incident Management	How well do we detect, accurately identify, handle, and recover from security incidents?	• Mean Time to Incident Discovery • Number of Incidents • Mean Time Between Security Incidents • Mean Time to Incident Recovery
Vulnerability Management	How well do we manage the exposure of the organization to vulnerabilities by identifying and mitigating known vulnerabilities?	• Vulnerability Scanning Coverage • Percent of Systems with No Known Severe Vulnerabilities • Mean Time to Mitigate Vulnerabilities • Number of Known Vulnerabilities
Patch Management	How well are we able to maintain the patch state of our systems?	• Patch Policy Compliance • Patch Management Coverage • Mean Time to Patch
Application Security	Can we rely on the security model of business applications to operate as intended?	• Number of Applications • Percent of Critical Applications • Risk Assessment Coverage • Security Testing Coverage
Configuration Management	How do changes to system configurations affect the security of the organization?	• Mean Time to Complete Changes • Percent of Changes with Security Reviews • Percent of Changes with Security Exceptions
Financial Metrics	What is the level and purpose of spending on information security?	• IT Security Spending as % of IT Budget • IT Security Budget Allocation

CIS Definition

Vulnerability Scan Coverage

Objective

Vulnerability Scan Coverage (VSC) indicates the scope of the organization's vulnerability identification process. Scanning of systems known to be under the organization's control provides the organization the ability to identify open known vulnerabilities on their systems. Percentage of systems covered allows the organization to become aware of areas of exposure and proactively remediate vulnerabilities before they are exploited.

Table 10: Vulnerability Scan Coverage

Metric Name	Vulnerability Scan Coverage
Version	1.0.0
Status	Final
Description	Vulnerability Scanning Coverage (VSC) measures the percentage of the organization's systems under management that were checked for vulnerabilities during vulnerability scanning and identification processes. This metric is used to indicate the scope of vulnerability identification efforts.
Audience	Management, Operations

CIS Measure

Question	What percentage of the organization's total systems has been checked for known vulnerabilities?
Answer	Positive integer value that is greater than or equal to zero but less than or equal to 100%. A value of "100%" indicates that all systems are covered by the vulnerability scanning process.
Formula	Vulnerability Scanning Coverage is calculated by dividing the total number of systems scanned by the total number of systems within the metric scope such as the entire organization: $$VSC = \frac{Count(Scanned\_Systems)}{Count(All\_Systems\_Within\_Organization)} * 100$$
Units	Percentage of systems
Frequency	Weekly, Monthly, Quarterly, Annually
Targets	VSC values should trend higher over time. Higher values are obviously better as it means more systems have been checked for vulnerabilities. A value of 100% means that all the systems are checked in vulnerability scans. For technical and operational reasons, this number will likely be below the theoretical maximum.

Make up our Mind

- Compliance
- Identification of “stuff”
- System Action
  - Hardening
- Incident Handling Improvement
- Mission Protection – hard to do when we rarely know what actually happened and what left the house.
  - Reduction of Data Loss
  - Reduction of IP loss
  - Prevention of mission compromise
- Risk Measurement and Metrics
- Cart before the horse
- WHAT IS THE PURPOSE?

Purposes

- Measure the problem
- Get people to fix things
- Get people to pay for things
- Get people to change the way they are doing things
- See if what you are doing is making a difference
- Move up in priority
- Satisfy compliance, IG, GAO, Regulators, the Hill, your boss
- Interesting fodder for the press

Making Metrics Actionable

1. Define the metrics program goals and objectives
2. Decide which metrics to generate
3. Develop strategies for collecting data that metrics will be based on
4. Develop strategies/models for generating the metrics
4. Establish benchmarks and targets
5. Determine how the metrics will be reported
6. Create an action plan and act on it, and
7. Establish a formal program review/refinement cycle

Failure of Current Cyber Metrics

- The lack of good estimators of system security.
- The reliance on subjective, human, qualitative (descriptive and subjective – as opposed to quantitative – numeric and precise) input.
- The current acceptance of bad metrics due to lack of knowledge
- Accepted use of very old taxonomy

Next Steps for Cyber Metrics

- Develop Formal Models of Security Measurement and Metrics
- Define both present and historical data collection and analysis process
- Measurement process
- Actionable Goals and Objectives
- Examine process regularly to ensure currency


mk·a
mischel kwon & associates llc