SAND2008-7991P

Red Team Metrics

A process for enhancing red team assessments with extended risk analysis

IDART

Information Design Assurance Red Team

Authored by John F. Clem, Dr. Mark Mateski, Raymond C. Parks, and Amy J. Shrouf

Presented by John F. Clem, Dr. Mark Mateski, and Amy J. Shrouf

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AI85000.

Course Outline

A **loose** schedule:

0730 – 0745	Sign-in and Continental Breakfast
0745 – 0845	Introductions and Course Introduction with RT Metrics Process Overview
0845 – 0900	Break
0900 – 0945	Section 1 – Identify Relevant Target Metrics
0945 – 1015	Exercise 1
1015 – 1115	Section 2 – Collect Data to Address Target Metrics
1115 – 1215	Lunch
1215 – 1245	Section 2 Exercise
1245 – 1315	Begin Section 3 – Analyze Risk Associated with the Target Metrics
1315 – 1400	SecureITree Demo and Section 3 Exercise
1400 – 1415	Break
1415 – 1500	Resume Section 3 Analyze Risk Associated with the Targeted Metrics
1500 – 1530	Section 4 – Assess and Communicate the Risk or Business Impact
1530 – 1600	Exercise 4
1600 – 1615	Open Discussion and Feedback

Introduction

- Course Objectives - why we’re here
- Definitions to get our brains started
- What metrics do for us (the value proposition)
- Early discussion on different aspects of metrics
  - what the experts have to say (good vs. bad),
  - how to measure the difficult to measure, and
  - etc.
- Red Team Metrics Process Overview

Course Objectives

- Perform our metrics process transfer through training,
  - work through the introduction to establish a common lexicon and framework for transferring our knowledge and process,
  - present our process in four sections, and
  - involve the students through discussion, exercises, and a demonstration
- Refresh concepts from RT4PM™ and IDART™ training that tie in to the metric work
- Have fun!

What is a Metric

Definitions

met·ric 2

(mĕt'rĭk) n.

A standard of measurement.

metric. Dictionary.com. *The American Heritage® Dictionary of the English Language, Fourth Edition*. Houghton Mifflin Company, 2004.

http://dictionary.reference.com/browse/metric

(accessed: August 18, 2008).

What is a Metric?

metric

noun

3.

a system of related measures that facilitates the quantification of some particular characteristic

[syn: system of measurement]

metric. Dictionary.com. *WordNet® 3.0*. Princeton University. http://dictionary.reference.com/browse/metric
(accessed: August 18, 2008).

What is a Metric?

Metric

A combination of measures, usually derived through a mathematical calculation involving two or more measures.

Pasted from

http://www.ic.gc.ca/epic/site/stcolevc.nsf/en/h_qw00037e.html

What is a Metric?

Metric: A measured value. For example, total sales is a metric.

Pasted from

http://www.1keydata.com/datawarehousing/glossary1.html

What is a Metric?

Metric

A measurement of a characteristic of an object or activity. The measurement is done using a consistent method, at consistent intervals, in order to assess, monitor and/or communicate information about the object or activity. Metrics may be quantitative or qualitative.

Pasted from http://www.esc.edu/personal/klf/kftest.nsf/webpages/handout.html

What is a Metric?

metric (*plural* **metrics**)

a measure for something; a means of deriving a quantitative measurement or approximation for otherwise qualitative phenomena (esp. used in Software Engineering)

Pasted from

http://en.wiktionary.org/wiki/metric

What is a Metric

The Definition of the Day - Ours

“A metric is a unit of measure and is used by analysts and decision makers to help measure important aspects of a problem of interest.”

What do Metrics do for us? (1)

- Measures and metrics provide a common language and direction for a program or project and frame the effort to collect the information needed to make informed decisions
- Kaydos argues that measurement/metrics
  - improve control [through feedback],
  - clarify responsibilities and objectives,
  - help align strategic objectives [strategic objectives lead to subobjectives which lead to measures],
  - understand business processes [you can't understand until you start to measure],
  - improve quality and productivity,
  - [people] defend their position

What do Metrics do for us? (2)

- Value Proposition – RT metrics are a measure of assurance for
  - functions,
  - processes, and
  - Systems
- Measures and metrics provide a common language and direction for a program or project and frame the effort to collect the information needed to make informed decisions

What Makes a Good Metric?

- Jaquith:
  - “a good metric should be
    - consistently measured, without subjective criteria
    - cheap to gather, preferably in an automated way
    - expressed as a cardinal number or percentage, not with qualitative labels like ‘high,’ ‘medium,’ and ‘low,’ and
    - expressed using at least one unit of measure, such as ‘defects,’ ‘hours,’ or ‘dollars’
  - a good metric should also ideally be contextually specific—relevant enough to decision-makers so that they can take actions” (22)

What Makes a Poor Metric?

Metrics are least useful when the following are true:

- They are inconsistently measured, usually because they are subjective
- They cannot be gathered cheaply
- They are expressed as high-medium-low ratings, grades, traffic lights or other non-numeric methods including ordinal numbers

Clarifying the Measurement Challenge

Guidance

- Hubbard writes, “Confronted with apparently difficult measurements, it helps to put the proposed measurement in context. Before we measure we should ask five questions:
  1. What is the decision this is supposed to support?
  2. What really is the thing being measured?
  3. Why does this thing matter to the decision being asked?
  4. What do you know about it now?
  5. What is the value to measuring it further?” (43)
- According to Kaydos, “The choice of the measurement technique to use should be based on the following factors:
  - What questions must be answered?
  - What techniques are feasible for producing the measure?
  - What is the most economical and reliable method of making the measurements?” (18)

Clarifying the Measurement Challenge

More Guidance

- Kaydos cites Galileo, who said “Count what is countable, measure what is measurable, and what is not measurable, make measurable.”

	METHOD	
REFERENCE	Direct	Indirect
Standardized	Measures of physical parameters and countable items	Determining physical measures by effects--deriving a planet's weight from its effect on another's orbit
Relative	Measures derived from countable items--complaints/sale, defects/car, inventory turns	Measures of qualities and abstract attributes--satisfaction, morale, helpfulness, kindness, honesty

“The standardized-indirect combination is interesting, because at first glance, it seems to be an impossible combination. However, scientists commonly use indirect techniques to measure physical parameters …” (17)

Sources for Previous Slides

- Jaquith is Andrew Jaquith, and citations reference his book, *Security Metrics* (2007), Boston: Pearson Education.
- Hubbard is Douglas W. Hubbard, and citations reference his book, *How to Measure Anything: Finding the Values of Intangibles in Business* (2007), Hoboken, NJ: John Wiley and Sons.
- Kaydos is Will Kaydos, and citations reference his book, *Operational Performance Measurement*: *Increasing Total Productivity* (1999), CRC.
- Non-cited material could be attributed to the IDART team and Dr. Mark Mateski of http://redteamjournal.com and to our colleagues with whom we have interacted and learned from over MANY years.

Red Team Metrics

- Help assessment stakeholders…
  - ⊛ understand the customer's business questions,
  - ① identify relevant target metrics,
  - ② collect data to address the target metrics,
  - ③ analyze risks associated with the target metrics, and
  - ④ assess and communicate the risk.

Process Overview

Understand the Customer’s Business Questions

- The customer wants to understand how adversaries might harm the customer’s business.
- Depending on the customer's preference, the RED TEAM LEAD may need to work with the customer to understand the customer's core business questions and relevant business impacts.

Process Overview

1

Targeted metrics

Identify Relevant Target Metrics

- The RED TEAM LEAD considers the customer's perspective, the types of red teaming involved, and the types of red teaming metrics available to identify the set of targeted metrics relevant to the assessment.
- It is assumed here that the RED TEAM LEAD already understands the CUSTOMER’s security questions and has identified the type of red teaming to be employed.

2

Collect data

Collect Data to Address the Target Metrics

- The RED TEAM applies the targeted metrics to the red team assessment process.
- The metrics specifically inform the task of collecting data during the assessment.

Process Overview

Analyze Risk Associated with the Target Metrics

- The RED TEAM analyzes risk based in part on the metrics identified and data collected relative to these metrics.

3

Analyze

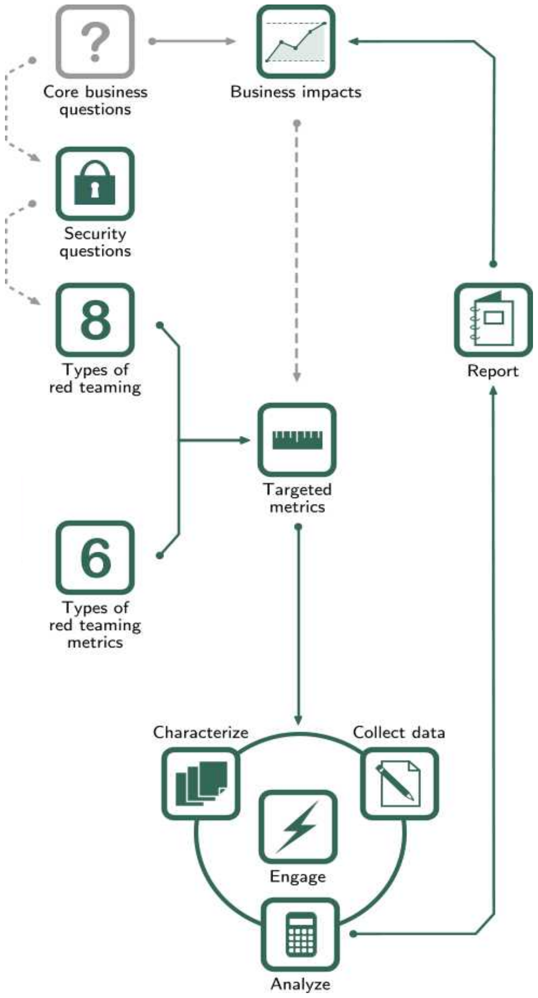
Assess and communicate the risk or business impact

- The RED TEAM LEAD assembles and delivers a report that communicates risk or business impact to the CUSTOMER.

4

Report

Process Overview



- The process maps to roles and responsibilities for THE SPONSOR and the REDTEAM.
- The RED TEAM LEAD has the biggest role in the use of this process

Questions?

Notes from Jaquith

- The following slides come from Andrew Jaquith, *Security Metrics* (2007), Boston: Pearson Education.

Some Key Thoughts

- “A metric is a consistent standard for measurement.”
- “The primary goal of metrics is to quantify data to facilitate insight.” (21)
- “As an analyst, I am keenly interested in making sure that persons examining a ‘metric’ for the first time should see it for what it is—a standard of measurement—rather than as something confusing that prompts a dissection of the measurer’s methods.” (22)

Notes from Hubbard

The following slides come from Douglas W. Hubbard, *How to Measure Anything: Finding the Values of Intangibles in Business* (2007), Hoboken, NJ: John Wiley and Sons.

Some Key Ideas

- Not every metric must be perfect; a good metric must simply *reduce* uncertainty
  - “The concept of measurement as ‘error reduction’ is a central theme of this book.” (17)
- Start with what you know
- If something really matters, it will generate some observable effect

Reasons why something can’t be measured

- These reasons are based on fallacies regarding
  - “*Concept of measurement*. The definition of measurement itself is widely misunderstood. If one actually understands what it means, a lot more things become measurable.”
  - “*Object of measurement*. The thing being measured is not well defined. Sloppy and ambiguous language gets in the way of measurement.”
  - “*Methods of measurement*. Many procedures of empirical observation are not well known. If people were familiar with some of these basic methods, it would become apparent that many things thought to be immeasurable are not only measurable but may already have been measured.”

Reasons why something shouldn’t be measured

- The measurement wouldn’t be cost-effective:
  - “The economic objection to measurement (i.e., any measurement would be too expensive).”
- The measurement wouldn’t be useful
  - “The general objection to the usefulness and meaningfulness of statistics (i.e., you can’t prove anything with statistics).”
- The measurement will be morally objectionable
  - “The ethical objection (i.e., we shouldn’t measure it because it would be immoral to measure it).”

The concept of measurement

- “For all practical purposes, the scientific crowd treats measurement as a set of observations that reduce uncertainty where the result is expressed as a quantity. A mere reduction, not necessarily elimination, of uncertainty will suffice for a measurement.” (21)
- “The practical differences between this definition and the most popular definitions of measurement are enormous. Not only does a true measurement not need to be infinitely precise to be considered a measurement, but the lack of reported error—implying the number is exact—can be an indication that empirical methods, such as sampling and experiments, were not used. Real scientific methods report numbers in ranges …” (21-22)

The concept of measurement

- “So measurement doesn’t have to eliminate uncertainty after all. A mere reduction in uncertainty counts as a measurement and possibly can be worth more than the cost of measurement.” (23)
- “But there is another key concept of measurement that would surprise most people: A measurement doesn’t have to be about a quantity in the way that we normally think of it. Note that the definition I offer of measurement says ‘where the result is expressed as a quantity.’ The uncertainty, at least, has to be quantified, but the subject of observation might not be a quantity itself—it could be entirely qualitative, such as a membership in a set.” (23)

The object of measurement

- “Even when this more useful concept of measurement is adopted, some things seem immeasurable because we simply don’t know what we mean when we first pose the question. We don’t really know what it is we want to measure: the object of measurement.” (24-25)
- “If I simply ask people what they mean and how it matters to them, they often answer the measurement question themselves.” (25)

The object of measurement

- The author suggests using what he calls the “clarification chain” to help identify the object of measurement:
  - “If it matters at all, it is detectable/observable.”
  - “If it is detectable, it can be detected as an amount (or range of possible amounts).”
  - “If it can be detected as a range of possible amounts, it can be measured.” (26)
- “The clarification chain is just a short series of connections that should bring us from thinking of something as an intangible to thinking of it as a tangible.” (26)

The method of measurement

- “Some things may seem immeasurable only because the person considering the measurement might not be aware of basic measurement methods—such as various sampling procedures or types of controlled experiments—that can be used to solve the problem. A common objection to measurement is that the problem is unique and has never been measured before , and there simply is no method that would ever reveal its value…. several proven measurement methods can be used for a variety of issues to help measure something you may have at first considered immeasurable.” (27)

The method of measurement

- “Measuring with very small random samples ...”
- “Measuring the population of things that you will never see all of …”
- “Measuring when may other, even unknown, variables are involved …”
- “Measuring the risk of rare events …”
- “Measuring the value of art, free time, or reducing risk to your life by assessing how much people actually pay for these things.” (27-28)

Four useful measurement assumptions

1. “Your problem is not as unusual as you think.”
2. “You have more data than you think.”
3. “You need less data than you think.”
4. “There is a useful

Economic objections to measurement

- “Perhaps the only valid basis to say that a measurement shouldn’t be made is that the cost of the measurement exceeds its benefits.” (33)
- “I’ve been calculating the economic value of measurements on every variable in dozens of various large business decisions. I found some fascinating patterns through this calculation, but, for now, I’ll mention just one: Most of the variables in a business case had an information value of zero. In each business case, something like one to four variables were both uncertain enough and had enough bearing on the outcome of the decision to merit deliberate measurement efforts.” (33)
- “… what really makes a measurement of high value is a lot of uncertainty combined with a high cost of being wrong.” (34)

A universal approach to measurement

- "Every component of this approach is well known to some particular field of research or industry, but no one routinely puts them together into a coherent method. In this universal approach, six questions need to be asked:" (39)

1. "What are you trying to measure? What is the real meaning of the alleged 'intangible'?" (39)
2. "Why do you care—what the decision and where is the 'threshold'?" (39)

A universal approach to measurement

3. “How much do you know now—what ranges or probabilities represent your uncertainty about this?” (39)
4. “What is the value of information? What are the consequences of being wrong and the chance of being wrong, and what, if any measurement effort would be justified?” (39)

A universal approach to measurement

5. “Within a cost justified by the information value, what observations would confirm or eliminate different possibilities? For each possible scenario, what is the simplest thing we should see if that scenario were true?” (39)
6. “How do you conduct the measurement that accounts for various types of avoidable errors (again, where the cost is less than the value of the information)?” (39)

Clarifying the measurement problem

- “Confronted with apparently difficult measurements, it helps to put the proposed measurement in context. Before we measure we should ask five questions:
  1. What is the decision this is supposed to support?
  2. What really is the thing being measured?
  3. Why does this thing matter to the decision being asked?
  4. What do you know about it now?
  5. What is the value to measuring it further?” (43)

Notes from Kaydos

- The following slides come from Will Kaydos, *Operational Performance Measurement*: *Increasing Total Productivity* (1999), CRC.

Why measure performance?

- In his first chapter, Kaydos outlines the advantages to managers of measuring operational performance. These advantages include the following:
  - “Improved control [through feedback],
  - Clear responsibilities and objectives,
  - Strategic alignment of objectives [strategic objectives lead to subobjectives which lead to measures],
  - Understanding business processes [you can’t understand until you start to measure],
  - Knowing what a process can do--its capability,
  - Improved quality and productivity,
  - More efficient allocation of resources,
  - The freedom to delegate,
  - Defending your position, and
  - Changing a company’s culture.”

Why measure performance?

- Kaydos also outlines benefits for employees. These include the following:
  - “Clear responsibilities and objectives,
  - Seeing accomplishments and receiving recognition,
  - Being evaluated objectively, and
  - More empowerment.”

What is measurement?

- Kaydos asserts that “Measurement consists of assigning a numeric scale to the size, value, or other characteristic of a tangible or intangible object. The scale could be as simple as 0 to 1 (bad or good), 0 to 10 (as in athletic competition), or a logarithmic scale like the Richter Scale …” (15)
- He also notes that all measures are relative: “A measure that is not referenced to something else has no meaning.” (15)

Standardized and relative measurements

- “When the reference for comparison is an internationally recognized standard, such as grams, meters, seconds, or volts, the measurement will be called *standardized* measurement. Countable items such as dollars, defects, or late deliveries can also be considered standardized because everyone agrees what a given number represents.” (16)
- “Where no accepted standard exists, the measure will be called a *relative* measure. A relative measure can be compared to itself as some other point in time or to the same measure in another system…. When using something other than a recognized standard as a basis for measurement, care must be taken to be sure any comparisons are valid.” (15)

Direct and indirect measurement methods

- “Once a reference for comparison has been established, how the measurement is going to be accomplished must be determined. If the object or condition itself is measured, the measurement is called *direct* measurement. Measuring the length of a board and counting rejected parts are direct measurements.” (16)
- “The other way something can be measured is to measure its effect rather than the item itself. This is called *indirect* measurement. For example, employee turnover and absenteeism can be indirect measures of morale. Even some physical qualities are measured indirectly. In a practical sense, using a meter to measure voltage is a direct measurement, but what is really being measured is the effect of the electricity, not the electricity itself.”
- “Most indirect measures could more accurately be called *indicators*, because while they will show a change in a variable, they may not provide a reliable measure of the degree of change. For example, if a satisfaction index goes from 10 to 20, we can be quite sure customers are more satisfied, but it would not be correct to say they are now twice as satisfied as they were before.” (16-17)

Direct and indirect measurement methods

	METHOD	
REFERENCE	Direct	Indirect
Standardized	Measures of physical parameters and countable items	Determining physical measures by effects--deriving a planet's weight from its effect on another's orbit
Relative	Measures derived from countable items--complaints/sale, defects/car, inventory turns	Measures of qualities and abstract attributes--satisfaction, morale, helpfulness, kindness, honesty

"The standardized-indirect combination is interesting, because at first glance, it seems to be an impossible combination. However, scientists commonly use indirect techniques to measure physical parameters …" (17)

Choosing the measurement method

- According to Kaydos, “The choice of the measurement technique to use should be based on the following factors:
  - What questions must be answered?
  - What techniques are feasible for producing the measure?
  - What is the most economical and reliable method of making the measurements?” (18)

Measuring intangibles

- "Measuring intangible concepts is far more common than most people appreciate. [For example] The 'quality' or 'appeal' of television programs is measured by the Nielsen index …. Even highly subjective factors like the quality of ice-skating and movies are routinely measured by knowledgeable judges in these fields. While someone may find fault with any particular instance, these measures are reliable guides once the user understands what they represent…. " (19)

Categories of performance measurements

- "In a broad sense, 'measurement' means assigning a number to a property on an object. In the simplest case, a measure could have two values, zero or one. The values assigned to a variable can be established by means such as counting, measuring with instruments, panels of judges, and other methods. In addition, to the characteristics already described, performance measures can e put into the following categories:
  - Qualitative or subjective—When numbers on a scale are assigned by human judgment. This does not necessarily imply there is any bias in the measure.
  - Quantitative or objective—When measures are derived from physical measurements or countable units.
  - Attribute—When a characteristic, such as a defect, is measured as either being present or not.
  - Variable or continuously variable—When the degree or extent of a variable is measured on a continuous scale. The dimensions of a table top are variables; dents are attributes since they are counted as either being present or not." (19)

If it has an effect, it can be measured

- “It cannot be proven, but I believe anything can be measured to a useful degree, especially in a business environment. If something can’t be measured directly, it must have an effect, which can be measured. If a process has no intended effect, it is clearly not worth measuring in the first place.” (19-20)

Galileo

- Kaydos cites Galileo, who said “Count what is countable, measure what is measurable, and what is not measurable, make measurable.” (See page 20.)