Security Metrics: The Quest For Meaning

Marcus J. Ranum
mjr@tenable.com
Tenable Network Security, Inc.

Agenda

- What are Metrics (versus statistics and heuristics)
- Why keep them?
- How do you establish a metric?
- How do you keep it relevant?
- Critical Questions

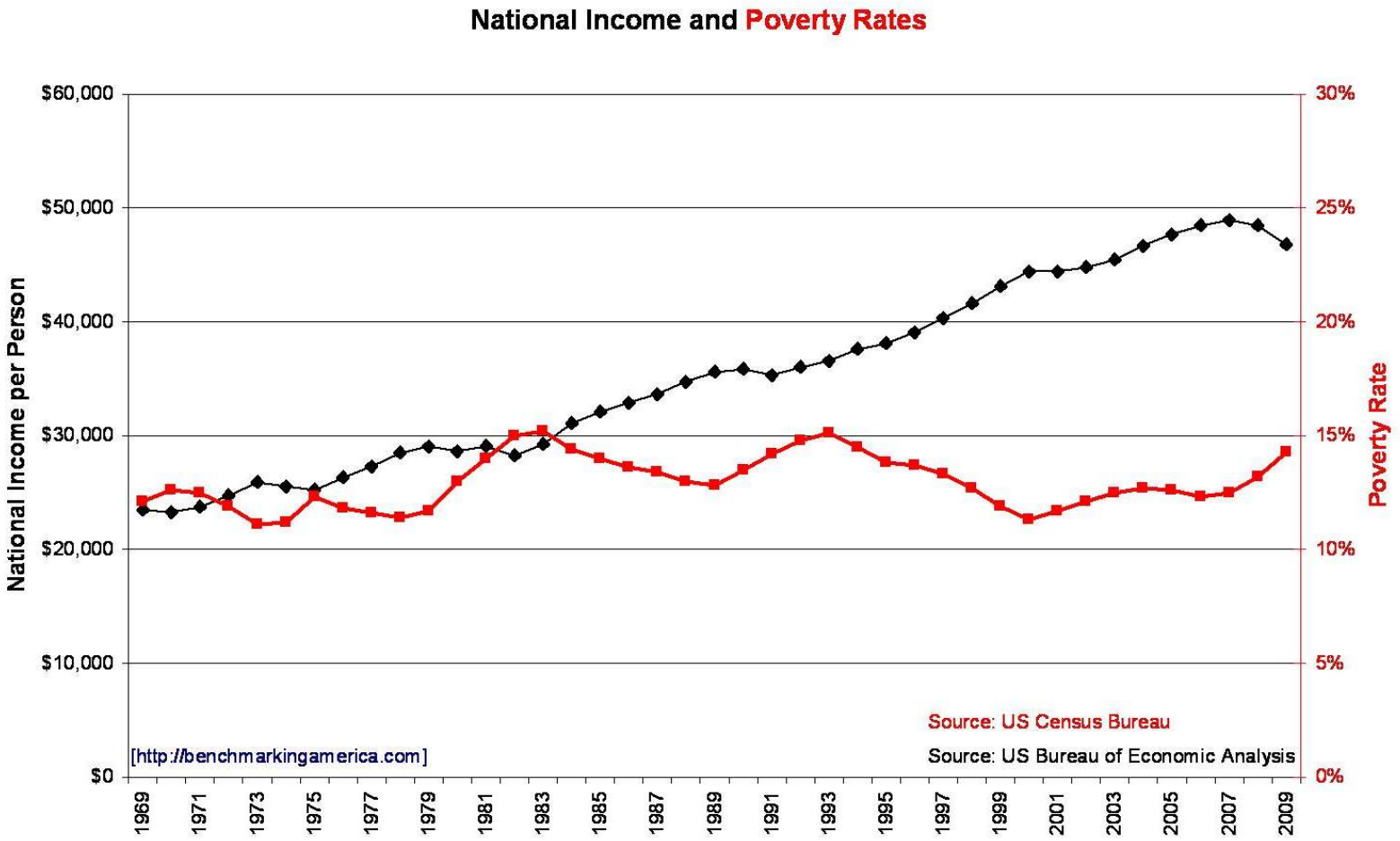
What are Metrics?

- A metric is some data and a means of reducing it to tell a story

Why Keep Metrics?

- To show you are succeeding
  - Corollary: to show you are failing
- To justify your existence and/or budget
- To argue for change
- For fun!

An Illustration



How To Establish Metrics

- Do not ask your boss

How Was the Poverty Line Established?

- ??

How To Establish Metrics

- Start with the question

How to Establish Metrics (2)

- Look at your process and make a list of what is quantifiable
- Ask yourself what quantities you are interested in
  - Once things are quantified they go up, or down - which is about the only convenient thing of metrics: they don't go sideways, too
- Which is a "good" direction: up or down?
- Do you know what constitutes a significant movement?
- Measure and iterate

Keeping Metrics Relevant

- Don't change your algorithm constantly
  - You are hitting yourself with a moving baseline; don't do that!
  - Or if you do, keep calculating the old metric and analyze it comparatively
  - If you need historical data draw a clear bar between what is collected and what is interpolated
    - (e.g: if you try to meld FTP transfer data with HTTP/HTTPS data how do you account for what happened in 1995 when HTTP completely blew FTP out of the water)
- Look at how you can build data atop more data

Keeping Metrics Relevant (2)

- Tying metrics to financial models is fraught
  - Always be honest about what is an extrapolation and what is data!
- The best kung fu for avoiding "metrics quagmire":
  Present your algorithm before you present data
  - Get buy-in on the algorithm first then the numbers speak for themselves!
- Tie things to existing known facts
  - Assuming a system admin fully loaded costs $200/hr and doing X will reduce time spent doing system restarts by 20%, take our existing rate and it'll save us Y$/year

Advanced Work

- You can generate subtle metrics if you can isolate a test-case
  - For some reason, this is considered "too hard" for many practitioners!
  - Consider: if you're hypothesizing that use of iPads to view PDFs and email would *reduce* email-borne malware rejection, try it on 20 volunteers for 6 months and compare the results against a normalized baseline!

Why Metrics Win

- Often information security becomes what I call a "battle of two narratives"
  - Your opponent has the advantage of lying: "moving this to the cloud will save us $500,000/year!"
  - To defend your narrative you need *facts* (from metrics) and *credible extrapolations* (based on metrics) or your opponent controls the narrative! *

* plan B is to respond with lies of your own

Critical Recommendations

- Establish a metrics process
  - Start by collecting the data you have
  - Examine it and determine what you *can* generate metrics about, with what you have
  - Examine your business processes and ask yourself where they can be quantified and measured at what critical junctions
  - Don't go overboard on statistics: keep them simple
  - Favor comparative metrics over absolutes ("last month we did X bleems per week, this month we did 4x")

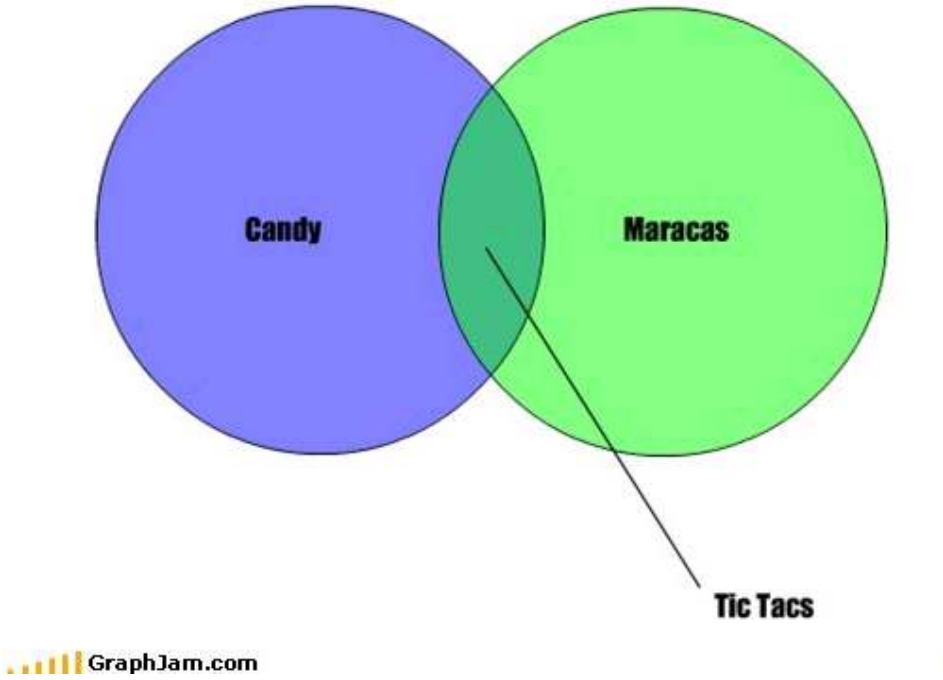
* plan B is to respond with lies of your own

Randomness

- Darrell Huff: How To Lie Statistics

Randomness

- Graphjam.memebase.com



Randomness

- http://okblog.okcupid.com/