RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: GRC-W10

Barney Fife Metrics: The Bullet That we Have but Don't Use, and Why

Jon Boyens

Manager, Security Engineering and Risk Management Group
National Institute of Standards and Technology

Celia Paulsen

Cybersecurity Researcher
National Institute of Standards and Technology

Disclaimer

The identification of any commercial product or trade name is included solely for the purpose of providing examples of publicly-disclosed events, and does not imply any particular position by the National Institute of Standards and Technology.

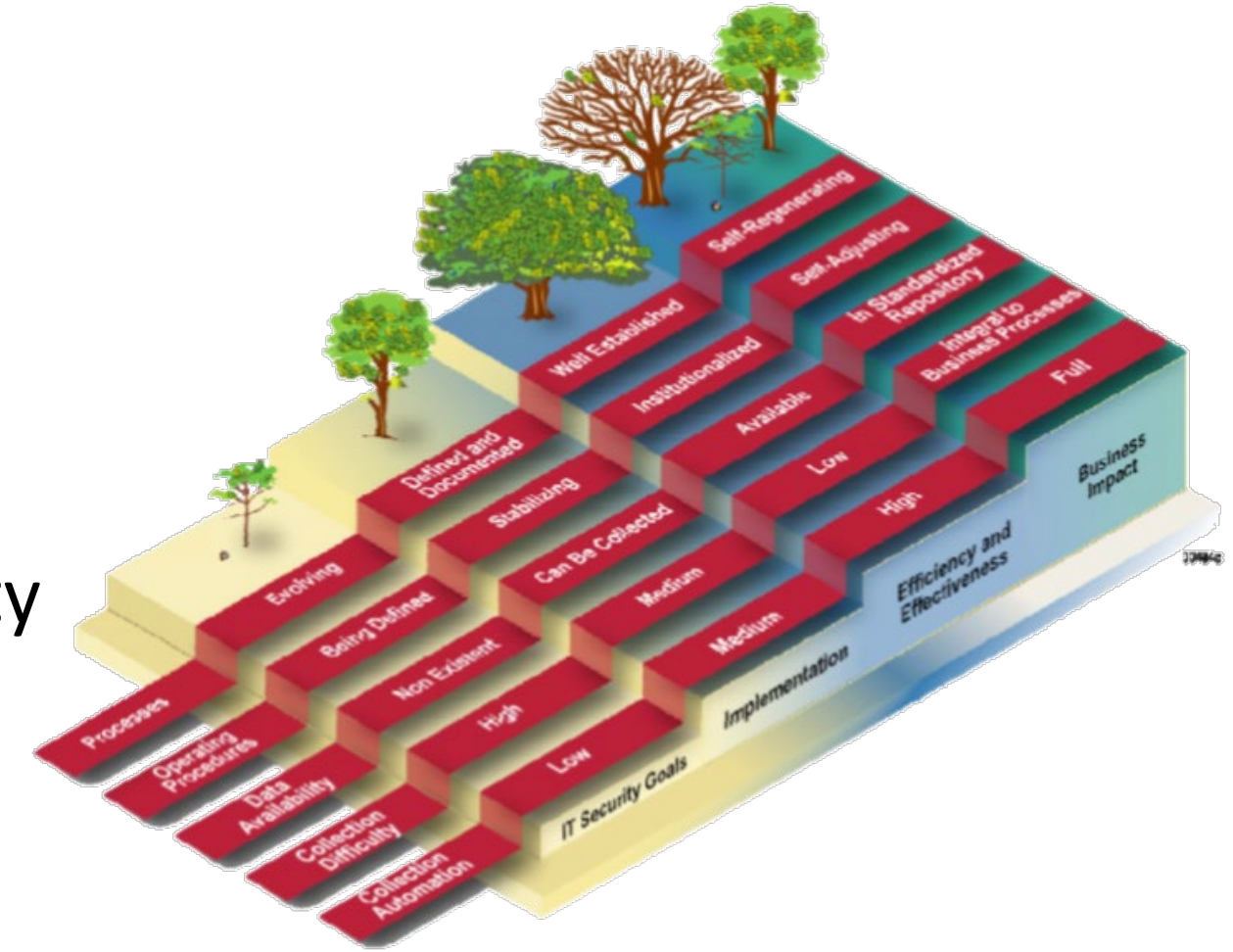
What's a Barney Fife?

And what does he have to do with metrics?

Image courtesy of Rogers and Cowan, Beverly Hills [Public domain], via Wikimedia Commons

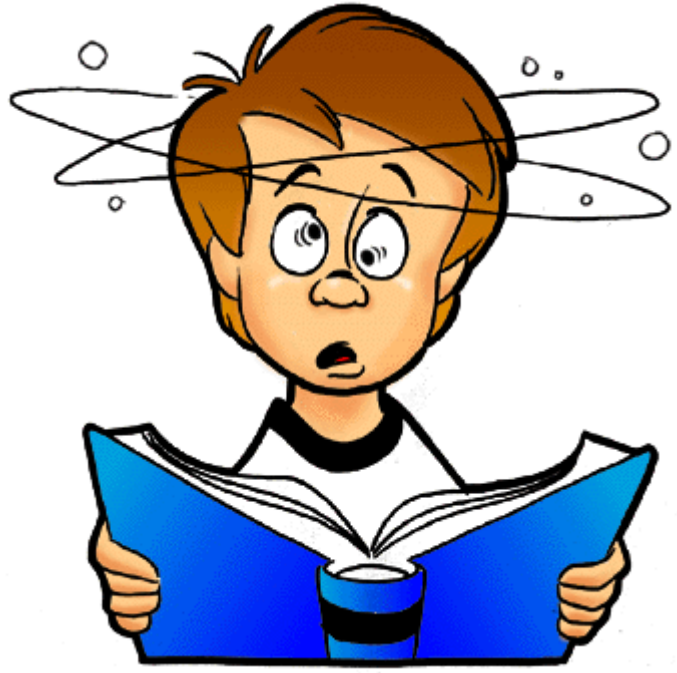
Question: it's been 20+ years: is there truly a lack of consensus and progress towards information security metrics maturity? If so, why?

- The Bullet
- Expected:
  - Industry shared solution(s)
  - Common set of practices
- Compare to financial or safety metrics



What we did

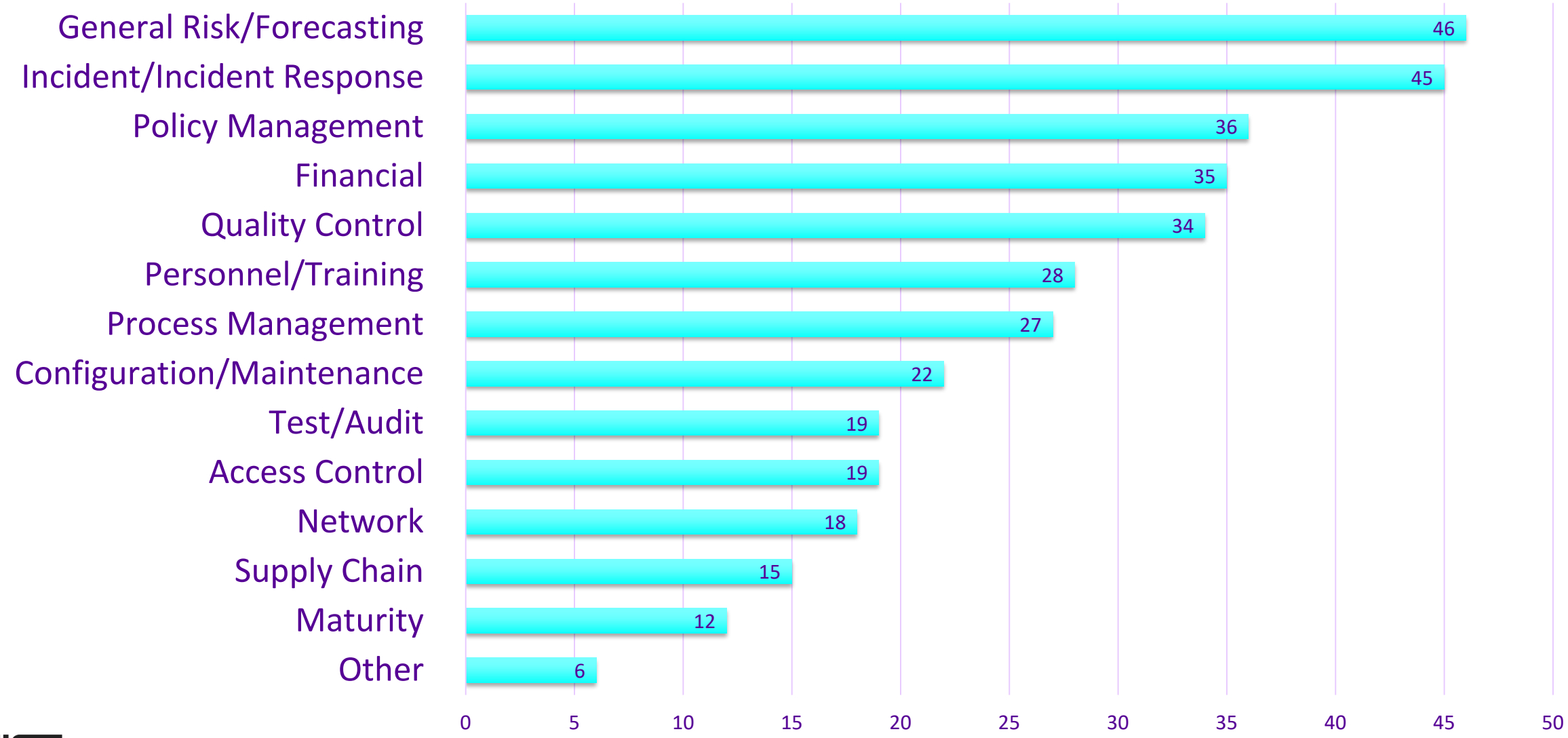
- Literature:
  - 160 Sources reviewed: 52 chosen
    - 28 on information security; 24 on related disciplines
  - 22 described metrics in enough detail
    - 429 total metrics; 373 unique metrics (87%)
- Interviews
  - 13 subject matter experts
    - Diversity in size, sector, regulatory oversight, etc
    - Senior information security & IT leaders (CIO, CISO, CSO, etc.)



Agenda

- State of maturity for cybersecurity metrics
  - Literature vs. Interviews
- Challenges to achieving maturity
  - Literature vs. Interviews
- Possible Best Practices
  - Literature vs. Interviews
- Where we go from here

Categories of Information Security Metrics in Literature

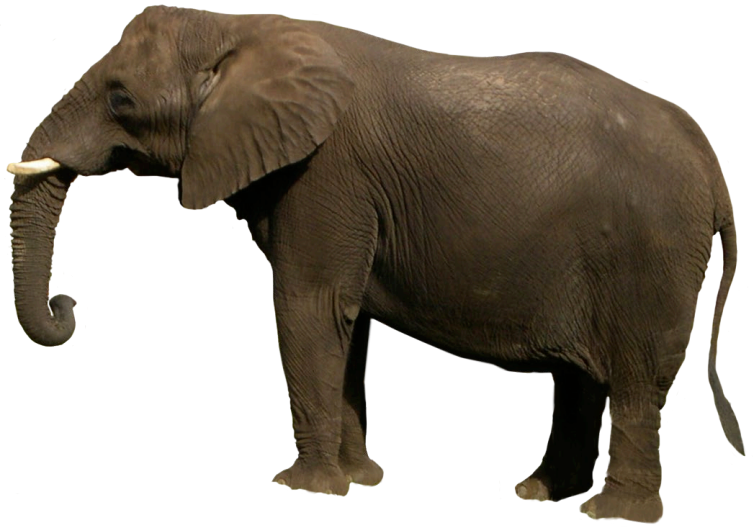


The State of Maturity of Cybersecurity Metrics

- Strategic (27%), managerial (53%), operational (20%)
- There is (still) a gap in the quality of managerial metrics (especially middle-management)
- Many programs seem to collect similar data, but mature programs use tailored metrics
- Mature programs evolve from measuring risk as a single metric to dynamically supporting business / project decisions

Questions Security Professionals Need to Answer

- What does good information security look like?
- What is the vocabulary we need to use to measure information security?
- How do we relate things to risk and to each other?



RSAConference2019

Challenges, Best Practices, and What's Next

Challenge #1: Too much data

- Early metrics programs collect and report fewer metrics
  - One-size-fits-all does not work
  - Number and frequency of reports decreased as programs matured
- Automation = more data (not necessarily better data)
  - Security tools
  - ERM / connected tools
  - Custom tools
- Filtering out the noise

Challenge #2: Simple vs. Complex

- Quality is more important than quantity
- Quality = (1) Easy to collect, (2) repeatable, (3) have value
  - Similar to literature
- Simple metrics are often not useful
  - e.g. Number of incidents
- Complex metrics are difficult to compile & make accurate
  - e.g. financial impact of risk

Challenge #3: Time & Commitment

- Finding a metrics champion
  - Must be able to translate board-level needs and priorities to data
  - Must be able to show how data can be useful in their world
- Even with executive support, resources, and talented leadership, takes time (e.g. six months for one organization)
- No such thing as “done”

Best Practice #1: Invest in a Program to Manage Metrics

- Metrics Champion
  - Understanding of data science & the business
- Make it a business priority
  - Make a program specifically for:
    - Identifying metrics
    - Testing metrics
    - Delivering metrics / reports
    - Improving metrics

Best Practice #2: Metrics Should "Tell a Story"

- Metrics tied to a goal
  - e.g. "security control effectiveness"; "Δ time"
  - Best if goal is strategic; if the metric can be used to direct strategic decision-making
- Measure trends and improvement, not numbers
  - More data does not necessarily mean better data
  - Show the meaning behind the number
- Need agreement on what a metric means and what action should they elicit

Best Practice #3: Experiment

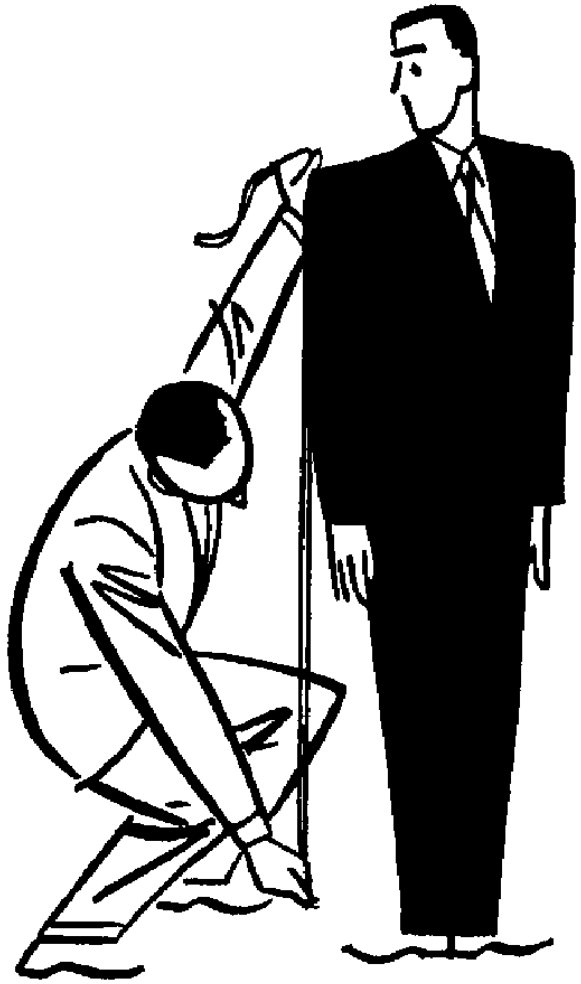
- Metrics programs need to be highly adaptive and dynamic
  - Rapidly evolving threats
  - Diverse and changing tools market
  - Changes in leadership priorities
- Different people need different information
- Start small
- Measure the effectiveness of your measurements!

Early vs. Mature Metrics Programs

Early Programs	Mature Programs
Use only pre-packaged metrics	Build on pre-packaged metrics
Everybody receives the same metrics	Metrics customized to function
Reporting the same info many times	Reporting changes & anomalies
Reporting more often	Reporting less often
Using simple metrics	Using complex metrics
Operational metrics only	Operational, managerial, & strategic
Create metrics once	Constantly improving metrics
Metrics as an after-thought	Metrics as key strategy driver

Research Needed

- Useful executive-level metrics
- KSAs for driving metrics programs
- Case studies:
  - Example metrics
  - How metrics are tested
- How to tailor information security metrics



The bullet we have but don't use

"Data! Data! Data! I can't make bricks without clay!"

– Sir Arthur Conan Doyle's Sherlock Holmes

Apply What You Have Learned Today

- Next week:
  - Identify a metrics champion for your organization
  - NIST SP 800-55 Rev. 1, Performance Measurement Guide for Information Security
- In the next three months:
  - Make a list of the data sources you have access to
  - Measure the effectiveness of your current metrics
  - Define what stories you need to hear/tell
- Within six months:
  - Have a core set of metrics for each layer of the organization
  - Create a program to test-drive metrics
  - Share your results!

RSAConference2019

Questions???

- Jon Boyens
- jon.boyens@nist.gov

- Celia Paulsen
- celia.paulsen@nist.gov

scrm@nist.gov