



YOUR SECURITY METRICS ARE LYING (AND WHAT TO DO ABOUT IT)

Mark Orlando, Bionic Cyber



ABOUT ME

21 years in cyber defense

Co-founder & CEO, Bionic Cyber

Former White House, DoE, CTO Raytheon Cyber

SANS Instructor, SEC450: Blue Team Fundamentals
and Security Operations and Co-author,
MGT551: Building and Leading Security Operations



WHY WE'RE HERE

Measuring security operations can be difficult, but we must get it right!

We're going to discuss common metrics that rarely tell a complete or compelling story and why they fall short.

We're also going to talk about ways to devise more meaningful metrics that promote the right behaviors.

WHAT IS A METRIC?



A MEASURE

A tool used to measure a business process

A PERFORMANCE INDICATOR

A tool to track how a specific function is performing; includes the current value and the target or threshold value, e.g. Key Performance Indicator (KPI)

PROGRESS TOWARD A GOAL

Objective or target state, plus key results you need to achieve the target state, e.g. Objectives and Key Results (OKR)

A STATUS CHECK

Metrics should tell you if ops are within normal/expected parameters, if you're achieving your goals

COMMON SECURITY METRICS



DETECTED INTRUSIONS

How many times have we been targeted?

How many threats did we mitigate before there was an impact?

INCIDENT RATES

Incident breakdown by severity level, attack vector, identification/response/recovery time, etc.

VULNERABILITY PATCH TIMES

Amount of time to update following patch release

RISK LEVEL

Risk expressed as a function of attack impact x likelihood

WHAT MAKES A GOOD SECURITY METRIC?



TOP-DOWN ALIGNMENT

Traceable to an objective or goal for your security team; tells you if the security team is meeting its commitments

CONSISTENT MEASUREMENT

Gathered without subjective criteria, preferably in a cheap/automated way

CORRECT APPLICATION

Used as an indicator, not a method of control

EXPRESSED AS A UNIT OF MEASURE

Expressed as percentage, hours, dollars, etc.

COMMON METRICS ISSUES:

1. TYPE ERRORS

Applying numeric labels to nominal or ordinal measures, and attempting to compute those labels

2. METRICS FIXATION

Using metrics as a replacement for judgement, experience, and talent



TYPE ERRORS IN SECURITY METRICS

FOUR MEASUREMENT TYPE CLASSIFICATIONS:^{1,2}

NOMINAL

Named

*e.g. colors, flavors,
towns*

ORDINAL

Named and Ordered

*e.g. satisfaction ratings,
education levels*

INTERVAL

Named, Ordered, with
Units of Even Spacing

e.g. temperature

RATIO

Same as Interval with Absolute
Zero

e.g. dollars, mass

[1] https://en.wikipedia.org/wiki/Level_of_measurement#Stevens's_typology

[2] Stevens, S. S. (7 June 1946). "On the Theory of Scales of Measurement".
Science. 103 (2684): 677–680



OPERATIONS ALLOWED FOR EACH MEASUREMENT¹

Incremental progress	Measure property	Mathematical operators	Advanced operations	Central tendency
Nominal	Classification, membership	$=, \neq$	Grouping	Mode
Ordinal	Comparison, level	$>, <$	Sorting	Median
Interval	Difference, affinity	$+, -$	Yardstick	Mean, deviation
Ratio	Magnitude, amount	$\times, /$	Ratio	Geometric mean, coefficient of variation

[1] https://en.wikipedia.org/wiki/Level_of_measurement#Stevens's_typology



CONSIDER THE RISK MATRIX

Impact and Likelihood are assigned a number (maybe 1-3), then we multiply to assess risk and color each cell accordingly

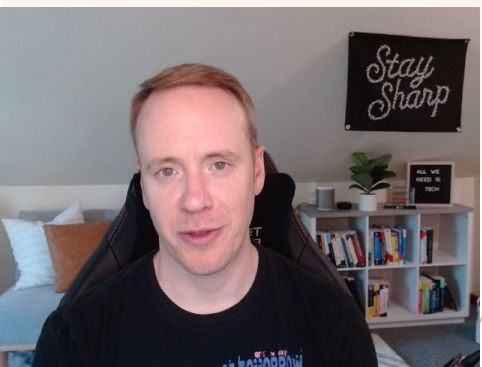
Likelihood	Impact				
	Negligible	Minor	Moderate	Significant	Severe
	Very Likely	Low	Moderate	High	High
	Likely	Low	Moderate	Moderate	High
	Possible	Low	Low	Moderate	Moderate
	Unlikely	Low	Low	Moderate	Moderate
	Very Unlikely	Low	Low	Low	Moderate

Source: <https://itsecurity.uiowa.edu/resources/everyone/determining-risk-levels>





QUESTIONS TO ANSWER:


1. Where did the numbers come from?
2. What unit of measurement are we using?
3. Is there a quantitative difference between a 1 and a 2? A yellow and red?



CONSIDER ALERT PRIORITIES

Vendor assigns numeric scores based on various factors, then computes those scores to get an overall Offense rating

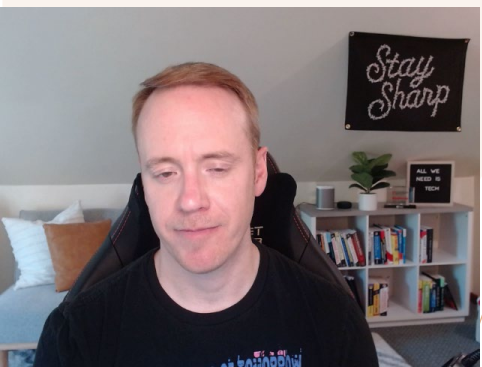
Status	 	Relevance	0	Severity	5	Credibility	3
Offense Type	Source IP						
Event/Flow count	<u>28 events</u> and <u>0 flows</u> in						
Start	Apr 21, 2019, 6:51:31 AM						

Offense 146
Magnitude




QUESTIONS TO ANSWER:

1. How would your team likely interpret an Offense with the highest score?
2. Did someone who knows and understands your environment set these priorities?
3. How do we know this math is meaningful?



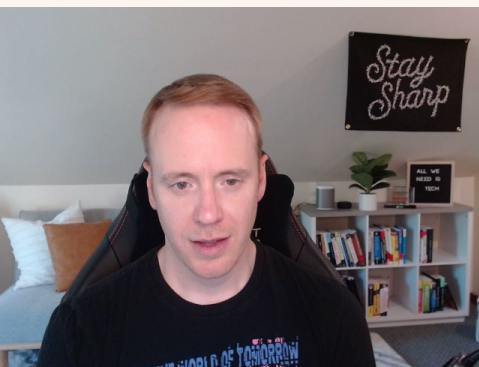
WHAT'S THE ISSUE HERE?

PROBLEM # 1

Qualitative labels – “medium, low, critical, important” – are assigned a number which implies interval/ratio data

PROBLEM # 2

Calculations based on numeric labels can't meaningfully be done when the measure is actually a nominal or ordinal!



AVOIDING TYPE ERRORS IN METRICS

1. USE THE RIGHT MEASUREMENT SCALE

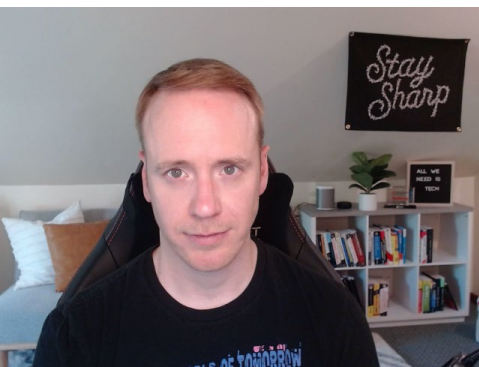
If you want to use interval/ratio values, design your metric that way from the start

2. DROP THE NUMBERS FOR ORDINALS

Create a mapping for ordinal measures to expected actions/responses instead of assigning values and performing calculations

3. SHIFT TO QUANTITATIVE ANALYSIS

Use probability and confidence intervals to create loss exceedance curves, compare to risk tolerance
(see Hubbard and Seiersen's book at the end of this deck)



METRICS FIXATION

“Not everything that can be counted counts, and not everything that counts can be counted.”¹

1. An attempt to replace management judgement, experience, and talent with numeric indicators

2. A belief that making metrics more transparent assures accountability

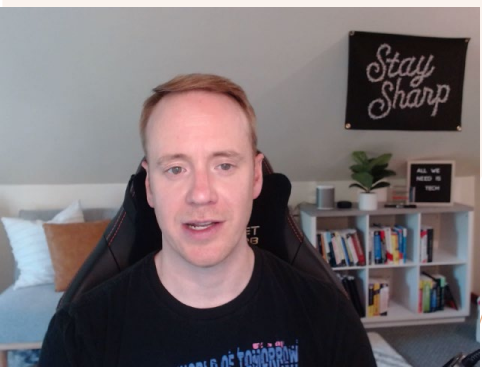
3. Tying individual rewards and penalties to measured performance to motivate people



[1] Chris Lorenz, “If You’re So Smart, Why Are You Under Surveillance? Universities, Neoliberalism, and New Public Management,” *Critical Inquiry* (Spring 2012)

COMMON METRICS FIXATION MISTAKES

1. Measuring the most easily measurable: simplifying problems by focusing on data most easily captured; closely related: materialist bias
2. Measuring inputs instead of outcomes (not the same as using leading indicators!)
3. Degrading information quality by “cleaning” (standardizing, normalizing) it



CONSEQUENCES OF METRICS FIXATION

GOAL DISPLACEMENT

When rewards and penalties are attached to metrics, people will focus on satisfying the metrics rather than the right behaviors

SHORT-TERMISM

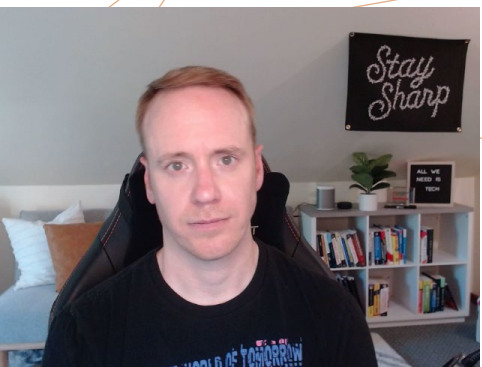
Focusing more on short-term goals than long-term success

SQUASHING INNOVATION

When performance is evaluated solely based on metrics, people are less likely to innovate and take risks that may result in metrics violations

DISCOURAGING COOPERATION

Individual or team rewards promote competition over cooperation, especially in multi-team systems like security organizations



WHY WE KEEP DOING THIS

ASSUMING CORRELATION IS CAUSATION

We assume there is an unknown, numeric variable that correlates with our ordinal measures

If true, vague guessing could be better than nothing...?

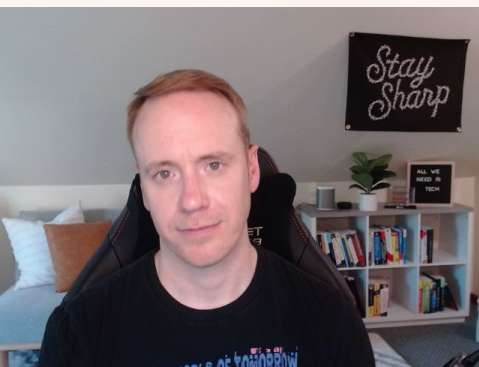
MERE- EXPOSURE EFFECT

We frequently see something, so it feels like it must be correct

Numbers make us feel safe and scientific, imply objectivity

“EASY BUTTON” FOR INFO OVERLOAD

Tempting way to deal with matters beyond one’s comprehension or time constraints



AVOIDING METRICS FIXATION

1. ENSURE FIT FOR PURPOSE

Diagnostic tool for security practitioners or reporting to others who may not grasp technicalities or limits?

2. GET INPUTS FROM THE RIGHT PEOPLE

Teams should buy into the purpose and validity of metrics just as much as the audience for those metrics; maybe more so if you want to reinforce intrinsic motivation

3. RECOGNIZE LIMITS OF DATA & TRANSPARENCY

Even the best metrics are subject to corruption and “gaming” – metrics must inform judgement, which includes how much weight to give them



TOP-DOWN ALIGNMENT

Start with high-level security goals, ask clarifying questions to understand what success looks like, and select the most useful metrics to track those results; commonly known as the *Goal-Question-Metric (GQM)* approach

PICK THE RIGHT DATA

Continuously revisit and assess your metrics; “measurement is not an alternative to judgement – measure *demands* judgement.”¹

CONSIDER THE NARRATIVE

What story are you trying to tell?
Focus on that narrative more than simply satisfying the metrics.

COVER LESS FOR GREATER IMPACT

Gathering and analyzing metrics has an opportunity cost and potentially a performance cost if used for reward/penalty. Focus on the most meaningful measures.

GET TEAM BUY-IN

“A system of measured performance will work only if those being measured believe in its worth.”²

A BETTER WAY

[1,2] Jerry Muller, *The Tyranny of Metrics*



GETTING STARTED

1. **Start with goals or objectives:** meaningful, important actions or results that have clear value to the business.
2. For each goal, come up with questions whose answers will tell you if the goal is being achieved.
3. Source the data you need to answer the questions.
4. Ensure the metric will inform some decision, conveys status quo or necessary action, and covers improvements as well as ongoing activities.
5. Discuss with your team(s) and hold them accountable, but use behaviors and outcomes to drive incentives – not numbers.



EXAMPLE

GOAL: Minimize the impacts of supply chain attacks

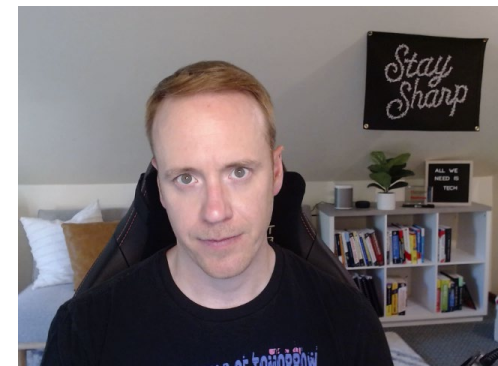
- **Question:** How do we define “supply chain attack”?
- **Question:** Do we have telemetry to monitor for those threats?
- **Question:** How are we capturing failures of supply chain risk mitigations?
 - **Metric:** Number of insertion attacks and third-party compromises in incident management system
 - **Metric:** Completion rate of third party attestations
 - **Metric:** Time to contain insertion attacks and third-party compromises



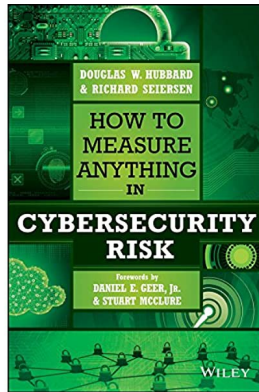
SUMMARY

Metrics are management tool that informs judgement, experience, and talent – it is not a replacement for those things.

Understanding how to select useful metrics and avoid common pitfalls like type errors and metrics fixation can enhance team focus and motivation.



REFERENCES



How to Measure Anything in Cybersecurity Risk

Douglas W. Hubbard

Richard Seiersen



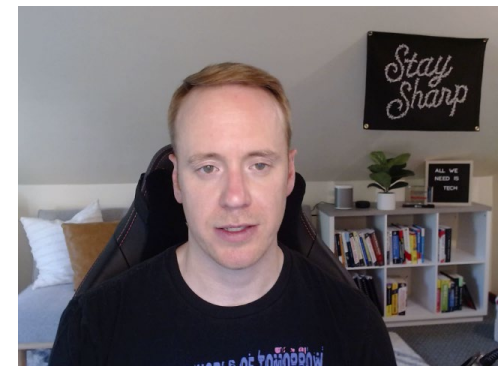
The Tyranny of Metrics

Jerry Z. Muller



SANS MGT551: Building and Leading Security Operations Centers

John Hubbard and
Mark Orlando





THANK YOU

Mark Orlando

<https://www.bionickeyber.com>

 <https://www.linkedin.com/in/marko16>

 <https://twitter.com/markaorlando>

