Money$ec

Applying the lessons of "Moneyball" to Information Security

Brian Keefer
Security Architect
Leading SaaS Security Company

Jared Pfost
Chief Executive Officer
Third Defense

Objective

- Show that
  - analytics revolutionized baseball
  - the same can be done w/InfoSec
  - you should give a rat's ass

What is Moneyball?

- Book by Michael Lewis
- Wrote books about financial markets
- Applies same analysis to baseball
- Baseball is just another market

How Analytics Changed Baseball

Oakland A's

- Teams bid for players in Free Agent market
- Start of 2002 A's had payroll ~$40M*
- NY Yankees payroll ~$126M*
- So poor teams have no shot at winning, right?

*From "Moneyball"

1999-2001

Team	Wins	Losses	Est Payroll*
NYY	280	203	$257M
OAK	280	205	$70M

*Estimate from baseball-reference.com

Billy Beane

- GM Billy Beane defied convention
- i.e. he didn't follow "best practices"
- made data-drive decisions
- Hired Paul DePodesta

Paul DePodesta

- Harvard econ grad
- Modeled value of On-Base Percentage
  - Value far above "conventional wisdom"
- Valued college players over highschool
- Helped shape investment strategy

Traditional baseball

- Teams sign players who
  - Look good
  - Hit/throw the ball hard
  - Run fast
  - Are aggressive

Traditional baseball

- Talent is evaluated by scouts
- Scouts are usually washed-up players
- i.e. “Industry veterans” or “experts”
- Value statements are largely subjective

Traditional baseball

- The favored "objective" measurements
  - Thrown-ball velocity (fastball MPH)
  - Average hits per official at-bat (AVG)
  - Balls dropped (E)

Next-gen Baseball

- Started in 1977
- Bill James wanted to see what influenced game outcome
  - Realized stats created in 1859 didn't properly attribute events

Sabermetrics

- Realized information collected & shared was inadequate
- Started collecting their own info
- Allowed them to create new stats to represent performance

Key lessons

- Don't make emotional decisions
  - At least recognize your bias
- Collect the "right" data
  - Look for correlations
- Set reasonable criteria for success
  - Don't overspend

This Applies to InfoSec

Problem statement

- Every organization is competing with attackers
- Most don't have Fortune 50 budget
- How can you be effective?

Conventional "wisdom"

- "Everyone knows" that you need
  - Firewall
  - Anti-virus
  - to change passwords frequently
  - prohibit social networking
  - etc

Do they work?

- Port 80 goes through the firewall
- Anti-virus misses custom malware
- Stolen passwords used quickly
- Social networking key to marketing and employee satisfaction

Clearly this is not working

- Do we actually want a new strategy?
- What would a new strategy look like?
- How do we get started?

Does management want to win?

- Data-driven
  - or data hidden?
- Make sure you're empowered to succeed

http://www.sox1fan.com

PG&E briefing warned of major risk of gas disaster

Pacific Gas and Electric Co.'s top officials were warned two months before the San Bruno pipeline explosion that gaps in the utility's gas system records, upkeep and emergency response plan created an "unacceptable risk" of a disaster, documents recently filed with state regulators show.

http://articles.sfgate.com/2011-08-07/news/29860613_1_president-chris-johns-peter-darbee-pg-e

What's our motivation?

- Incidents, findings, etc.
- Do they know what Winning is?
  - E.g. process avoiding **material loss** in the most **efficient** manner

Material Loss?

- Post mortems
- Risk Assessments

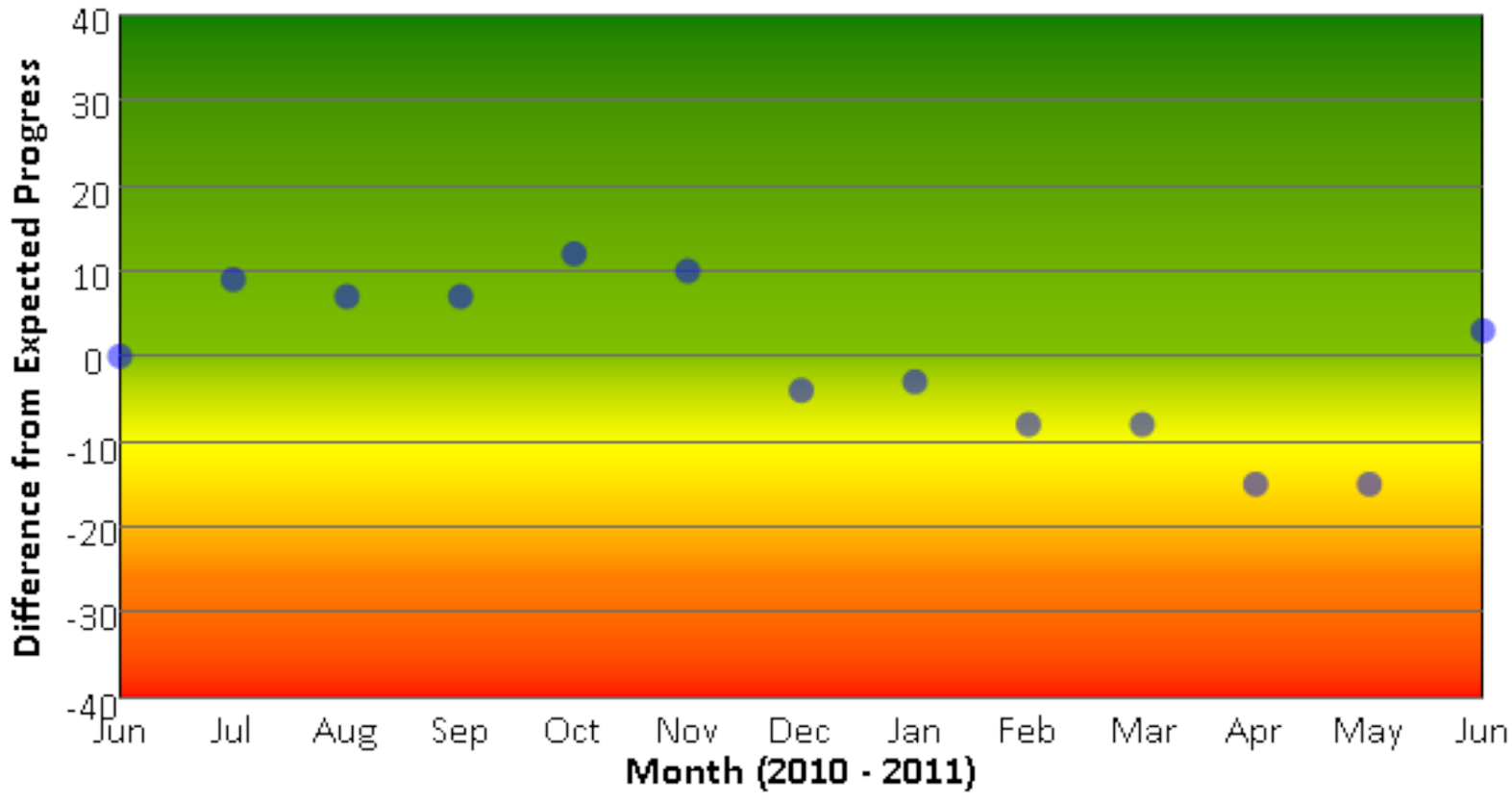
Efficient?

- Control Effectiveness
- Team Efficiency

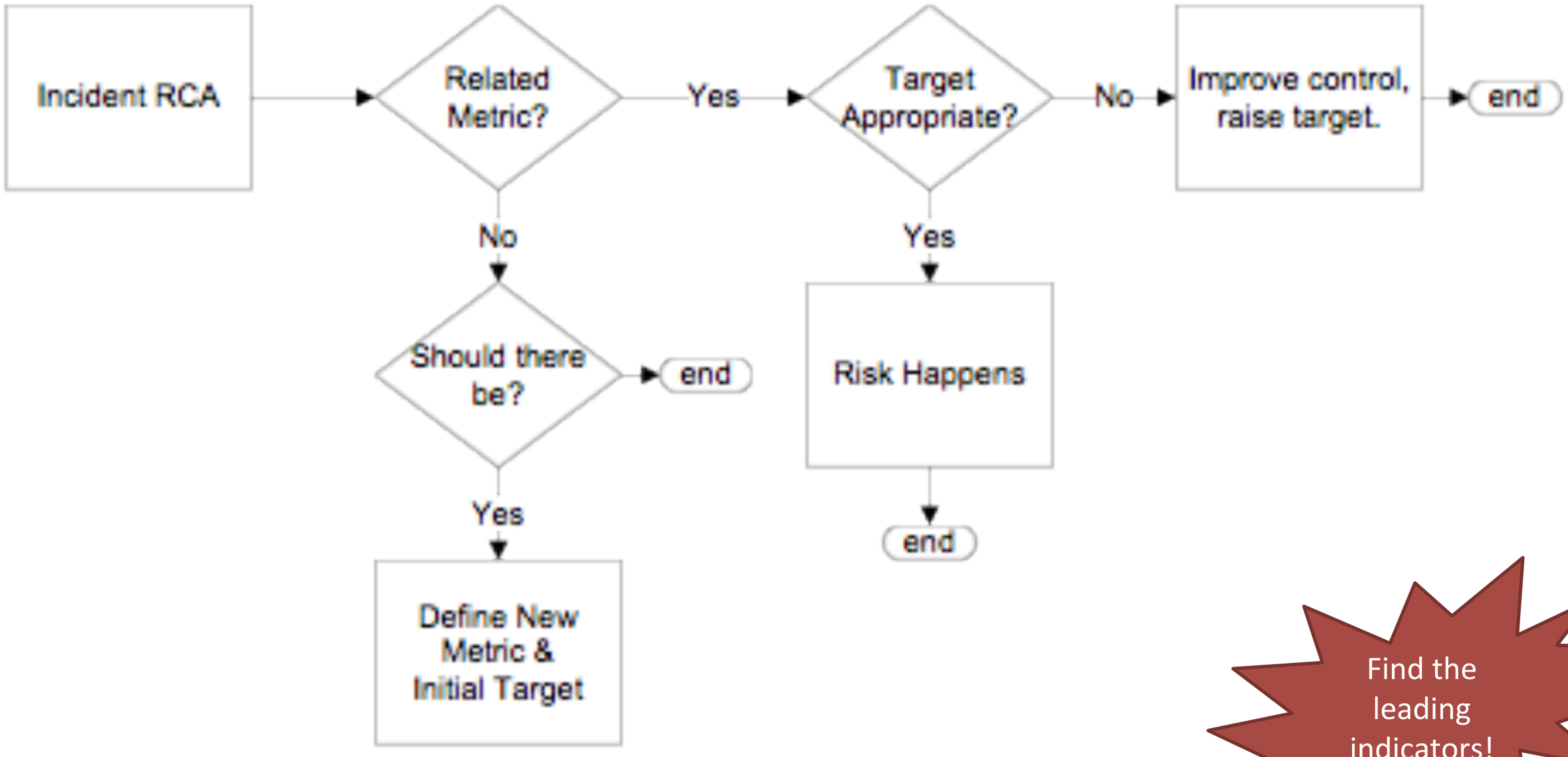
- Which metrics correlate with winning?

Real Metrics Have Outcomes

- Stats are trendy, Metrics have Winners|Losers
  - Measure actual performance against target
  - Benefits
    - Drives “acceptable risk” conversation with Management
    - Simplifies reporting e.g. are we above|below?



Integrate Metrics Into Root Cause Analysis



Find the leading indicators!

Incident - Metric Correlation: Controls

- Candidate Metrics
  - –Device
    - Patch & config vulns (via scanner)
  - –Application
    - Post-production applications vulns
  - –Access Management
    - % Employee termination within policy
    - % Role/Access verification
  - –Network
    - % critical systems monitored

Incident - Metric Correlation: Controls

- Vendors
  - % assessed per policy
  - # overdue findings
- Employee
  - # of duplicate RCA's
- Change Management
  - # emergency or unplanned changes
  - % of changes with a regression
- Incident
  - # of <high> Business Impact Incidents

25

Incident - Metric Correlation: Efficiency

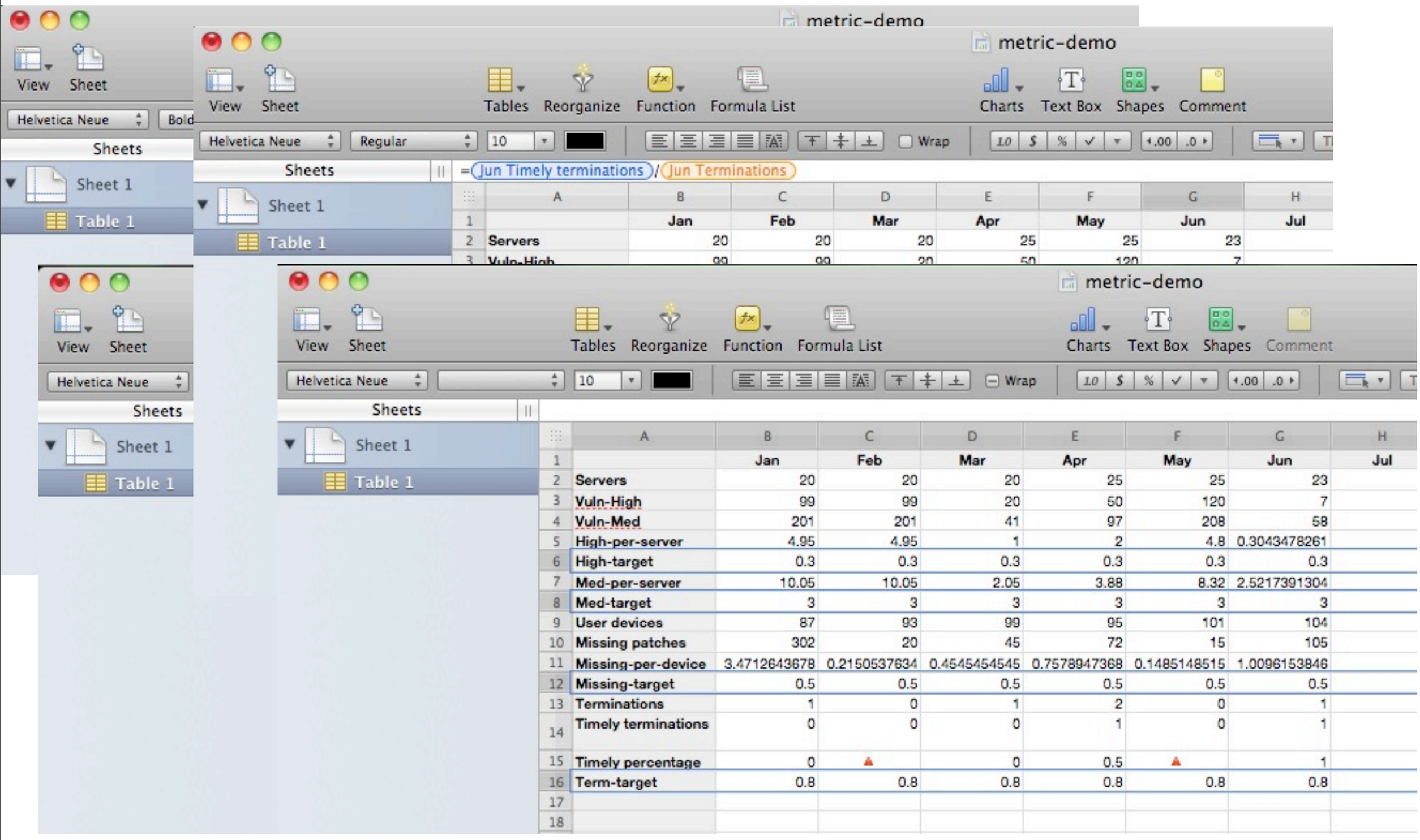
- Candidates
  - –% Processes with Role Definitions - RACI
  - –% Project Performance
  - –% Lines of Business with Risk Assessments
  - –Actual vs. Target maturity for key services
    - Assessment
    - Change Control
    - Incident Response
- Real-time, rather than after-the-fact surveys

Metric Status Table

Title	Status	Trend
Master Security Index	-8	↑
Business Risk Assessments	0	↑
Team Improvement	-10	→
Team SLA Coverage	-6	↑
Security Role Definition	-10	↑
Security Initiatives: On Time	-11	↓
Security Initiatives: On Budget	-11	↓
Internal Consulting Services	0	→
Audit Management	-10	→
Audit Mitigations Complete	-10	↑

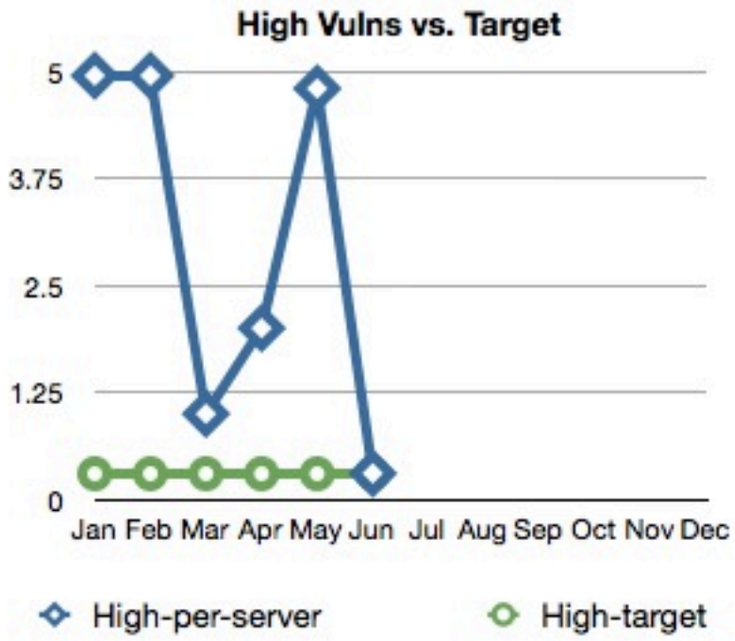
26

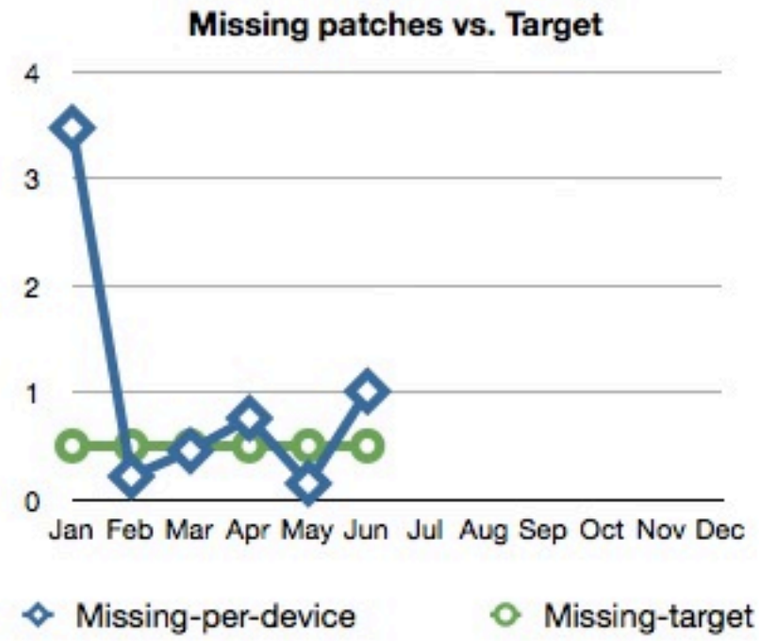
You really can do this

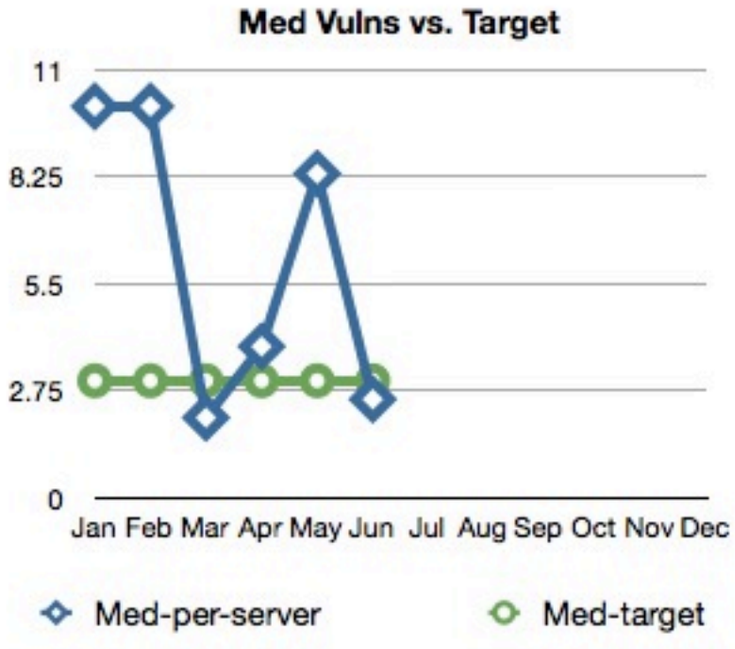


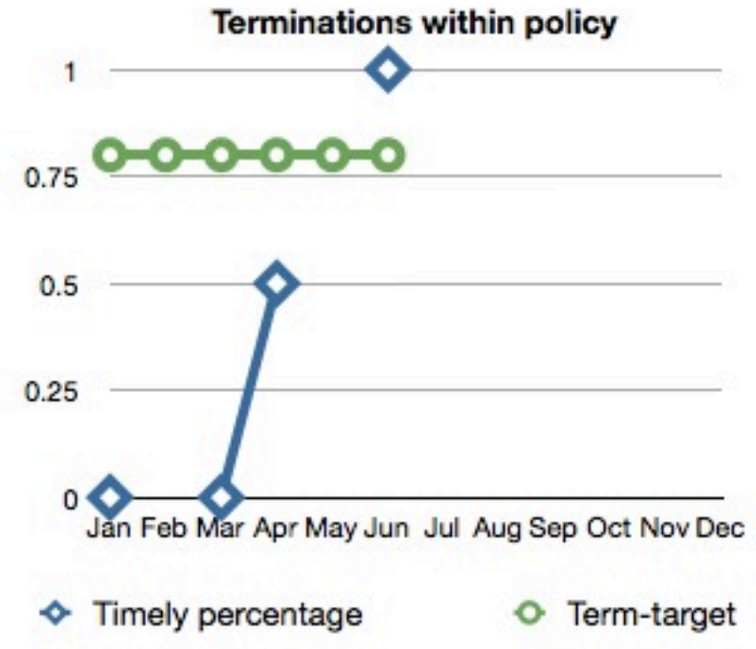
	A	B	C	D	E	F	G	H
1		Jan	Feb	Mar	Apr	May	Jun	Jul
2	Servers	20	20	20	25	25	23	
3	Vuln-High	99	99	20	50	120	7	
4	Vuln-Med	201	201	41	97	208	58	
5	High-per-server	4.95	4.95	1	2	4.8	0.3043478261	
6	High-target	0.3	0.3	0.3	0.3	0.3	0.3	
7	Med-per-server	10.05	10.05	2.05	3.88	8.32	2.5217391304	
8	Med-target	3	3	3	3	3	3	
9	User devices	87	93	99	95	101	104	
10	Missing patches	302	20	45	72	15	105	
11	Missing-per-device	3.4712643678	0.2150537634	0.4545454545	0.7578947368	0.1485148515	1.0096153846	
12	Missing-target	0.5	0.5	0.5	0.5	0.5	0.5	
13	Terminations	1	0	1	2	0	1	
14	Timely terminations	0	0	0	1	0	1	
15	Timely percentage	0	▲	0	0.5	▲	1	
16	Term-target	0.8	0.8	0.8	0.8	0.8	0.8	
17								
18								

Ooooh, shiny!


High Vulns vs. Target
5
3.75
2.5
1.25
0
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
High-per-server
High-target


Missing patches vs. Target
4
3
2
1
0
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Missing-per-device
Missing-target


Med Vulns vs. Target
11
8.25
5.5
2.75
0
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Med-per-server
Med-target


Terminations within policy
1
0.75
0.5
0.25
0
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Timely percentage
Term-target

Next

- Semi-annual comparison of incident vs. control effectiveness
- Right metrics?
  - Expand | Contract
- Didn't find correlation
  - Review Incident root cause analysis
  - Re-mix metric suite
- Found correlation
  - Analyze metrics e.g. optimal age of patching
    - Maybe we're spending too much...

Why You Should Care

Ever wonder why...

- Really smart people don't seem to get promoted
  - but someone who doesn't understand details does?
- People you know are moving up
  - but you aren't?

It's not random chance

- People who don't move beyond details are cursed to forever be lumberjacks
- robber barons know about forests

You can’t move past this

Unless you can make sense of this

Don’t take it from me

How to Kick Ass in Information Security — Hoff’s Spritually-Enlightened Top Ten Guide to Health, Wealth and Happiness

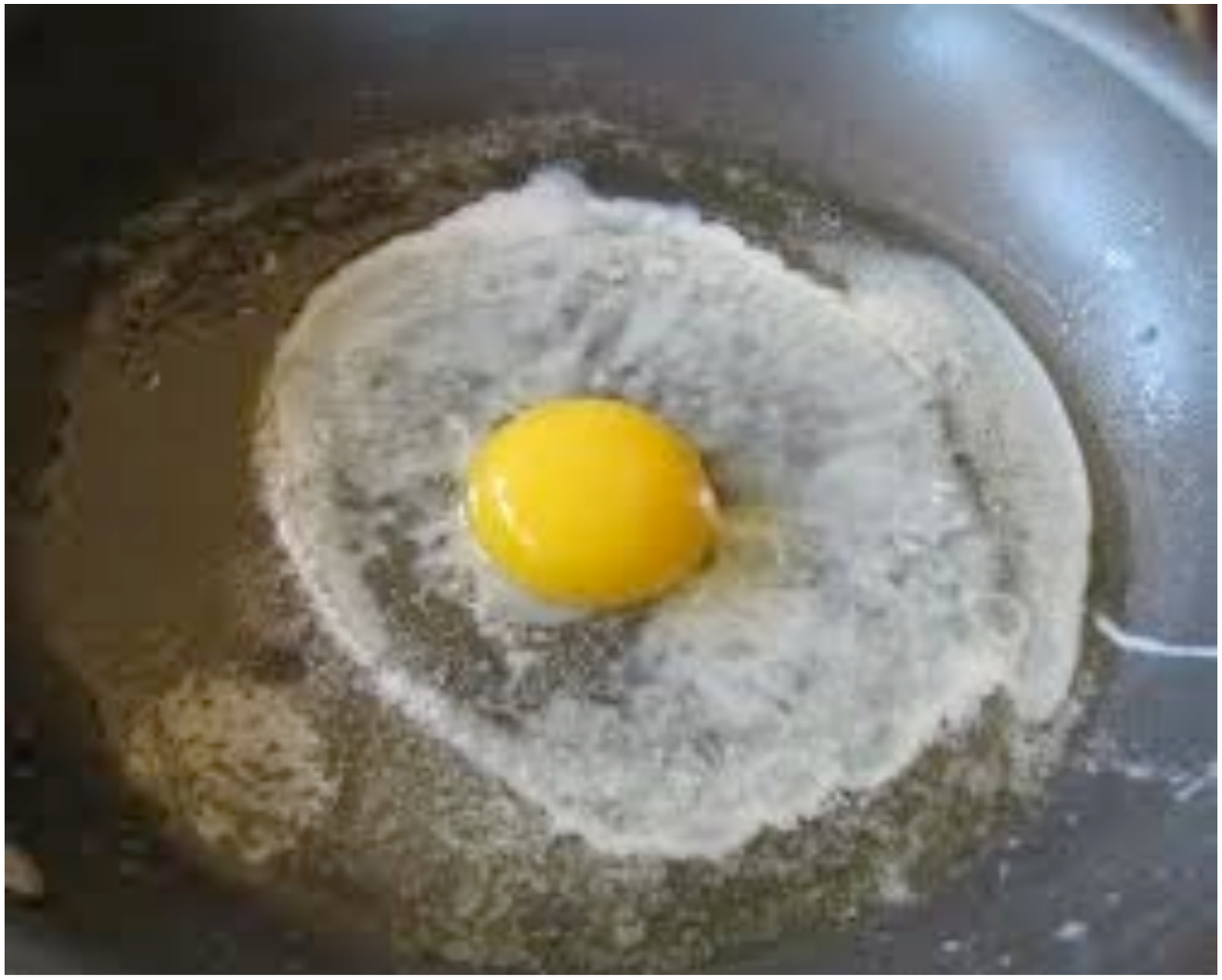
1. Measure Something

I don’t care whether you believe in calling this "metrics" or not. If you’ve got a pulse and a brain (OK, you probably need both for this) then you need to recognize that the axiom "you can’t manage what you don’t measure" is actually true, and the output – no matter what you call it – is vitally important if you expect to be taken seriously.

The bottom line

- If you want to be successful you need to
  - solve problems that matter
    - articulate when & why issues matter
    - measure how well you solved them
      - and what the benefit was
- Credibility is everything!

Any questions?



Thanks!

Brian Keefer

b: http://rants.smtps.net
e: chort@smtps.net
t: @chort0

Jared Pfost

b: http://thirddefense.wordpress.com
e: jared@thirddefense.com
t: @JaredPfost