

Security Metrics That *Matter*

Tanya Janca
CEO &
Founder



What are we going to talk about today?

The value of measurement, reporting and improvement

What and how to get metrics that truly *matter*

Example case studies that apply these lessons

Tanya Janca

- CEO & Founder @ We Hack Purple
- AKA @SheHacksPurple
- Author: **Alice and Bob Learn Application Security**
- 20+ years in tech, Sec + Dev
- WoSEC (Women of Security) founder
- OWASP Chapter and Project founder
- Blogger, Podcaster, Streamer, Builder, Breaker
- Nerd at Large



Metrics

“a method of measuring something, or the results obtained from this.”

The Value of Metrics



We measure so that
we can report and so
that we can improve.

Reporting is for
Management.

Improvement is for *us*.

Metrics and Reporting

Reporting helps us get budget for tools, other resources and staff.

Reporting is sometimes part of compliance/audit.

Reporting makes our bosses happy and is a box we need to check.

But what we need metrics for is improvement.

Metrics and Reporting

Reports are for bosses; metrics are for ***us***.

Vanity Metrics

Numbers that make us look good, but aren't actually *valuable*.

Vanity Metrics



Vanity Metrics



Vanity Metrics



Security Program Goals

Think about your security program goals.

Figure out what can help you get there.

Then measure it.

We will circle back to this.



Metrics \cong Measurement



Metrics – In House Risk Score

Based on:

- ease of exploit
- public/internal
- privilege gained
- how long the vulnerability has been known
- specific risks to your business
- data classification
- CIA affected?

Security Metrics That *Matter*

Metrics *That Matter*

- Time to detection
- Time to remediation and/or patch
- Baseline security posture, how close are you to your goals? How much closer 3, 6, 12 months later?
- Are **you** meeting your SLAs with developers and ops?
- Average number of vulnerabilities per system or app, and does this go down over time?
- Detecting the same types of vulns? Reduction in #s?
- Are you now able to detect new types of vulns?
- After education on specific topics do instances decline?
- After targeting specific vulns do they decline?

Security Incidents

The most expensive, humiliating and damaging way to deal with a vulnerability for the first time.

Reducing the number of incidents, the length of time to resolve, or damage they cause, is an extremely high value goal.



Incident Metrics *That Matter*

Measuring Incidents

- Time to resolve
- Time to detect
- Time to diagnose as incident or just event (triage)
- Types/categories of incidents
- Process is/is not followed
- Cost & damage
- Types repeated, or new types found
- Other teams understand what to do/cooperative
- Post-mortem performed *every single time*?
- Quarterly review of incident stats
- Time between incidents (if there's no recovery time that's an issue) — Note on resting your staff
- Access and tooling was/was not available








Tools for Measurement

Ability to see patterns and trends.

Ability to keep information safe.

Ability to automate data collection.


Tools for Measurement

- Excel 
- Email or documents in folders 
- Vulnerability Management tools 
- Checking several different security tool dashboards 
- Other tooling dashboards not meant for Vuln Management, such as Power BI and other Business Data tools 
- Your cloud dashboard if it accepts external info 
- Saving it all to a DB and querying it yourself 

Automate as much as humanly possible.

But this applies to everything in life. ;-D

Improvement!

A black and white photograph of a woman with long dark hair, wearing a dark cap and a jacket, sitting in a chair and working on a laptop. She is positioned in front of a large window that looks out onto a city skyline. The lighting is soft, coming from the window, creating a professional and focused atmosphere.

Think back to
your security
program goals
for these next
slides.

Improvement; Using Metrics

- Education on your top 3
- Bug type eradication
- Compliance (regs + your policies & standards)
- Are you meeting your SLAs? Bug Fixing SLAs?
- Are you repeating incidents? Finding new kinds?

Time for a Case Study

Improvement Case Study

Example Goal: Cut our incidents involving insecure software by half.

How do we get there?

- Reduce number of all incidents
- Make all software more secure
- Have better detection
- Have automated responses
- Have better trained IR staff

If we aren't measuring we don't know where to start.

Step 1:
Analyze the metrics you have

Improvement Case Study – Step 1

Example Goal: Cut our incidents involving insecure software by half.

- analyze all incident and post mortems for patterns
 - attack types, if you see a pattern then you can attack the entire pattern (if you have lots of XSS, give lessons on XSS)
 - Root cause – insecure code, no testing, advanced attacker?
 - Did everyone follow the IR Process, and if not, why not? Maybe it needs to be fixed?
 - Look for types of incidents, DOS, resource attacks, targeted attacks versus scanning tools, use of zero days, etc.

Improvement Case Study – Step 1

Example Goal: Cut our incidents involving insecure software by half.

- Time to resolve? Reasons it takes so long?
- How well does your team respond? Were there errors?
- How well did other teams respond? Did they follow the process? Did they know the process?
- Did your team have all the tools, resources and info they needed?
- How long did it take to detect?
- How long did it take to clean up?
- How much did it cost (hours/\$), total?

Step 2:

Gather missing metrics

(if possible)

Improvement Case Study – Step 2

New information from metrics and discussion:

- Zero days are really important to the executives, way more important than you realized
- Some incidents take a really long time to finish, it turns out how long they take is way more important than how many there are
- 35% of your incidents are caused by only 2 types of vulnerabilities
- Your APIs are being abused quite a bit, and it's causing crashes, unavailability and larger-than-necessary cloud bills

Step 3: Adjust goal based on metrics

Improvement Case Study – Step 3

Example Goal: Cut our incidents involving insecure software by half.

Readjust goal: at this point you may want to readjust your goal. Perhaps you want to have incidents resolved in ½ the time, and to stamp out one or two entire types of incident? See what's important to your executive and your team, and go from there.

Goals should be adjusted as we have new information.

Improvement Case Study – Step 3

Potential new goals:

#1 Reduce time responding to incidents by 50%

- Create and deliver team-specific training of what we need during an incident for helpdesk, system admins and software developers
- Update to IR process documentation, and sharing of this process widely
- Ensure your App inventory is complete, current, includes contact info, and also has a list of components and frameworks (use inventory tool plus an SCA tool for this)

Improvement Case Study – Step 3

Potential new goal:

#2 Be able to respond to zero days

- Implement WAF or RASP to be able to implement virtual patches in case of zero day being exploited in the wild

Improvement Case Study – Step 3

Potential new goal:

#3 Reduce overall number of AppSec incidents by 35% by eliminating top two bug classes found

- Top 2 vulnerability types found repeatedly in incidents to be stamped out completely via unit tests, scans and education program.

Improvement Case Study – Step 3

Potential new goal:

#4 Reduce resource abuse

- DOS protection
- Resource quotas & throttling on all APIs

Step 4: Create Game Plan

Improvement Case Study – Step 4

Steps to get there (your game plan!):

- Implement tool to deflect resource DOS attacks (or pay for service from cloud provider) and throttling and resource quotas on all APIs
- Implement WAF or RASP to be able to implement virtual patches in case of zero day being exploited in the wild
- Top 2 vulnerability types found repeatedly in incidents to be stamped out completely via unit tests, scans and education program.

Improvement Case Study **Game Plan**

Steps to get there (your game plan!):

- Team specific training of what we need during an incident for helpdesk, system admins and software developers
- Update to IR process documentation, and sharing of this process widely
- Ensure your App & API inventory is complete, current, includes contact info, and also has a list of components and frameworks (use inventory tool plus an SCA tool for this)


Improvement Case Study **Game Plan**

Steps to get there (your game plan!):

Review Incident Reports and Post Mortems for trends every quarter.

Using Metrics Changed
EVERYTHING about that goal.

For your consideration.

 Earn Points on this Purchase!

Measure What Matters

HOW GOOGLE, BONO, AND THE GATES FOUNDATION ROCK THE WORLD WITH OKRS

By John Doerr
Foreword by Larry Page

Best Seller

Category: **Management**

Hardcover

Hardcover \$27.00

ADD TO CART

Apr 24, 2018 | ISBN 9780525536222

Also available from:

Barnes & Noble

Books A Million

Bookshop.org

Hudson Booksellers

IndieBound

Powell's

Target

Walmart

Amazon

#1 NEW YORK TIMES BESTSELLER

Measure What Matters

How Google, Bono, and the Gates
Foundation Rock the World with OKRs

John Doerr

WITH A FOREWORD BY LARRY PAGE

READ AN EXCERPT

Look Inside

What did we learn today?

The value of metrics, and using them for reporting and improvement

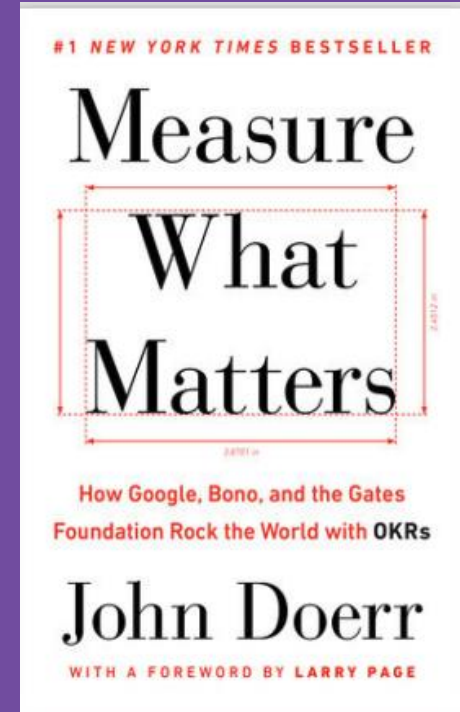
What and how to get metrics that truly *matter*

How to apply this information for best results!

Resources

Awesome Books

- The DevOps Handbook
- The Phoenix Project
- Accelerate
- The Unicorn Project



- Alice and Bob Learn Application Security

WoSEC – Women of Security

Women of Security (WoSEC) is a community for women, including LGBTQ+ women, non-binary, trans and gender nonconforming, who have an interest in cyber security.

We want women to join the information security community and have long-term, happy, careers.

<https://WoSEC.tribe.so>

<https://www.womenofsecurity.com>

@WoSECTweets

I have a podcast!!!!!!

We Hack Purple Podcast explores different careers in InfoSec and how you can get there! On all popular podcast platforms, or join us LIVE every Thursday at 6:00 pm PAC on YouTube!

<https://www.youtube.com/WeHackPurple>

#CyberMentoringMonday

Every Monday!

Resources: ME!!!!

Twitter: @SheHacksPurple

<https://dev.to/SheHacksPurple>

<https://YouTube.com/SheHacksPurple>
[e](#)

<https://SheHacksPurple.ca>

THANK YOU!



Tanya Janca

SheHacksPurple.ca

WeHackPurple.com