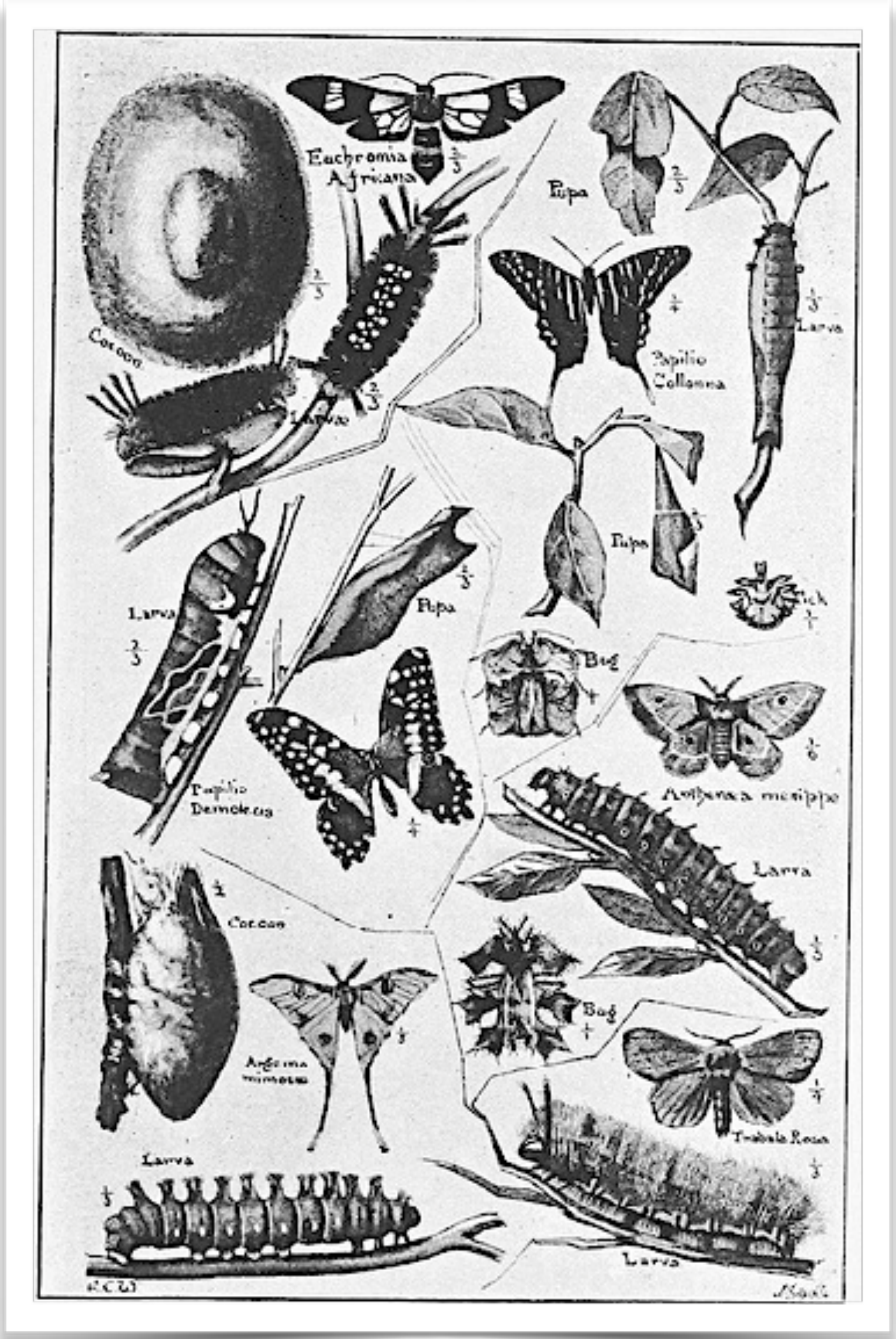
Evolving a Bug Bounty Program

SOURCE Seattle — October 13, 2016
Mike Shema

cobalt.io

An Insect Zoo

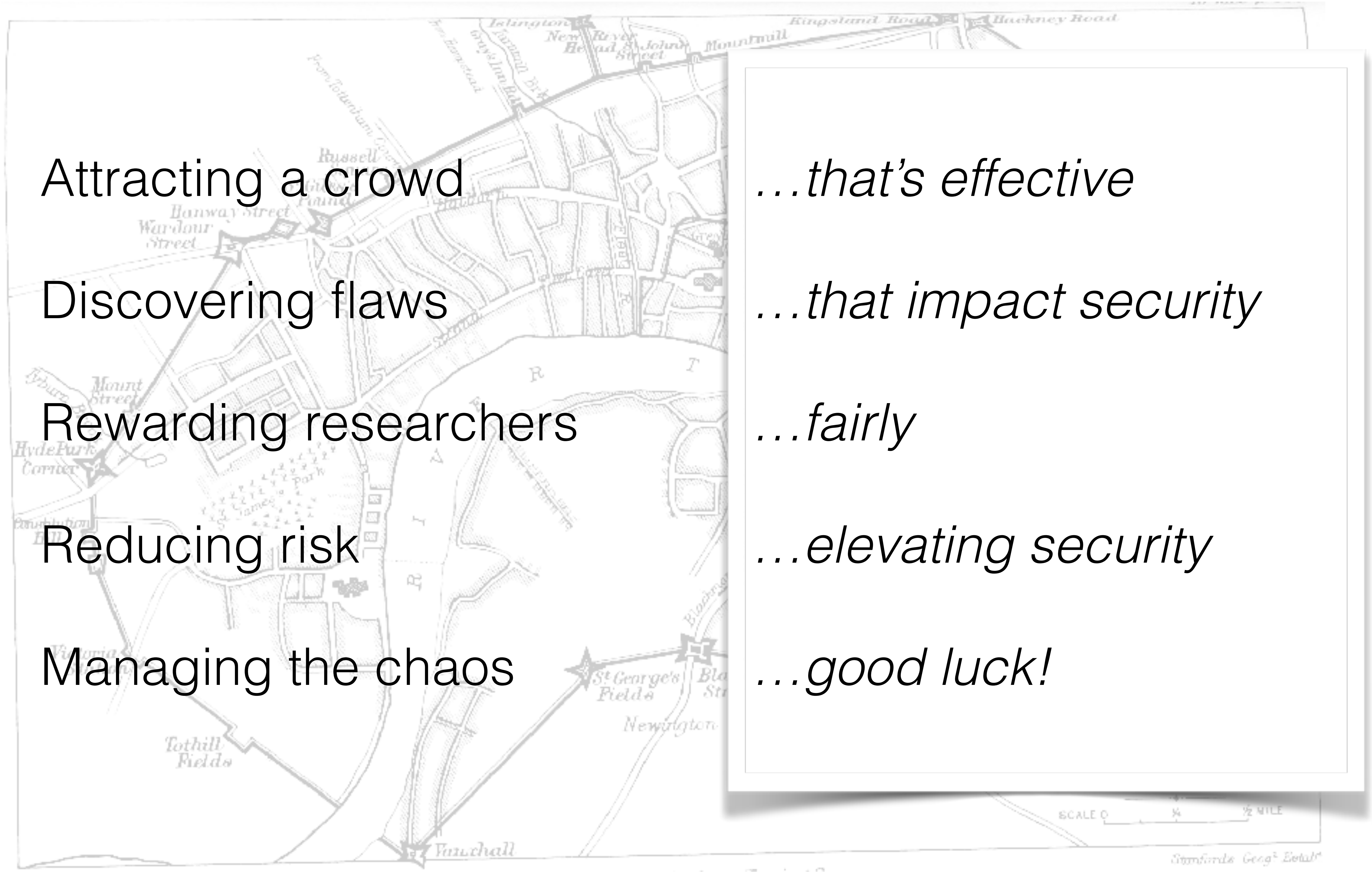


Bug Bounties embrace a crowdsource model for discovering application flaws.

They reward researchers for disclosing flaws in a way that minimizes risk to the app, its data, and its users.

…and they're a bit chaotic.

Plan Your Visit

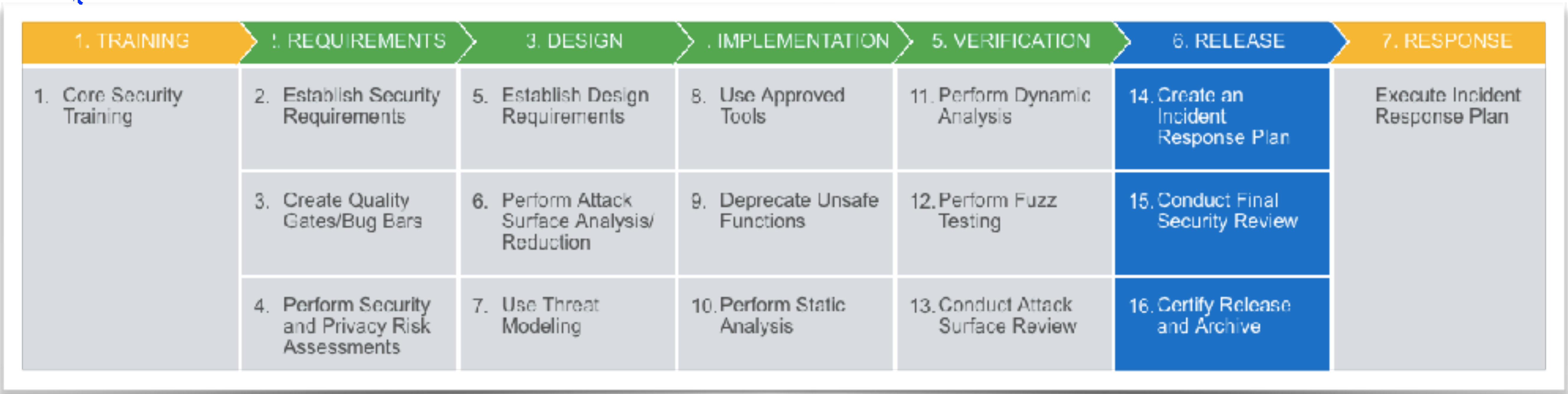


Attracting a crowd	*…that's effective*
Discovering flaws	*…that impact security*
Rewarding researchers	*…fairly*
Reducing risk	*…elevating security*
Managing the chaos	*…good luck!*

Find an Ecological Niche

The maturity of a security development lifecycle influences the success of a bug bounty program.

Descent with modification



1. TRAINING	!. REQUIREMENTS	3. DESIGN	. IMPLEMENTATION	5. VERIFICATION	6. RELEASE	7. RESPONSE
1. Core Security Training	2. Establish Security Requirements	5. Establish Design Requirements	8. Use Approved Tools	11. Perform Dynamic Analysis	14. Create an Incident Response Plan	Execute Incident Response Plan
	3. Create Quality Gates/Bug Bars	6. Perform Attack Surface Analysis/ Reduction	9. Deprecate Unsafe Functions	12. Perform Fuzz Testing	15. Conduct Final Security Review	
	4. Perform Security and Privacy Risk Assessments	7. Use Threat Modeling	10. Perform Static Analysis	13. Conduct Attack Surface Review	16. Certify Release and Archive	

https://www.microsoft.com/SDL

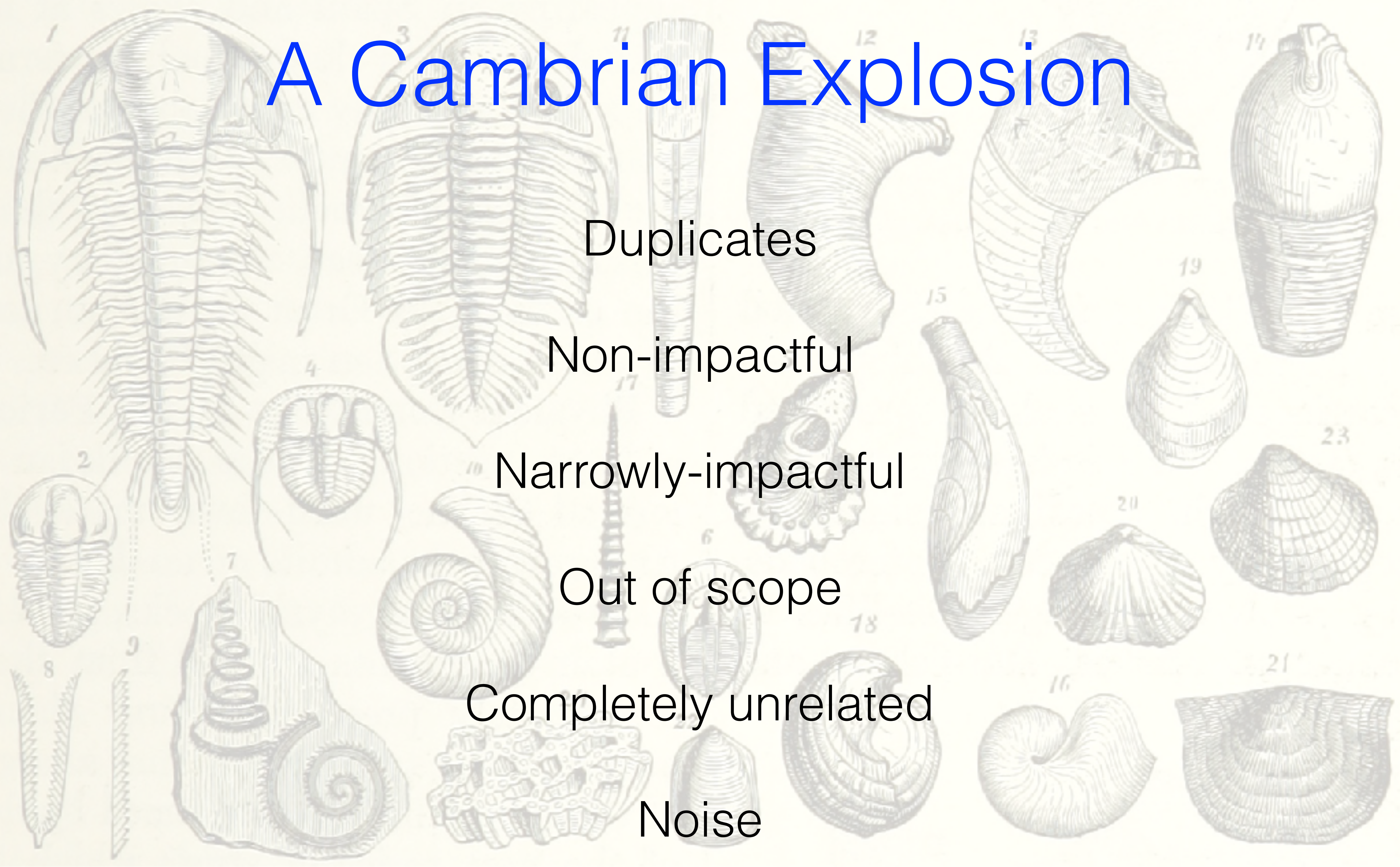
Encountering the Swarm

Be ready for a high rate of incoming reports that produce a low percentage of actionable bugs.

15+ / day

20% valid

A Cambrian Explosion



Duplicates

Non-impactful

Narrowly-impactful

Out of scope

Completely unrelated

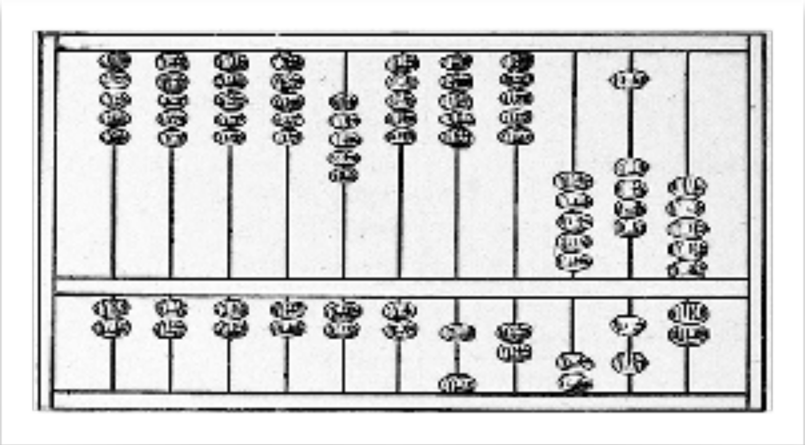
Noise

Environmental Pressures

Who determines impact? Who determines priority?

What is the SLA to acknowledge, verify, fix, validate?

What happens when the SLA is broken?

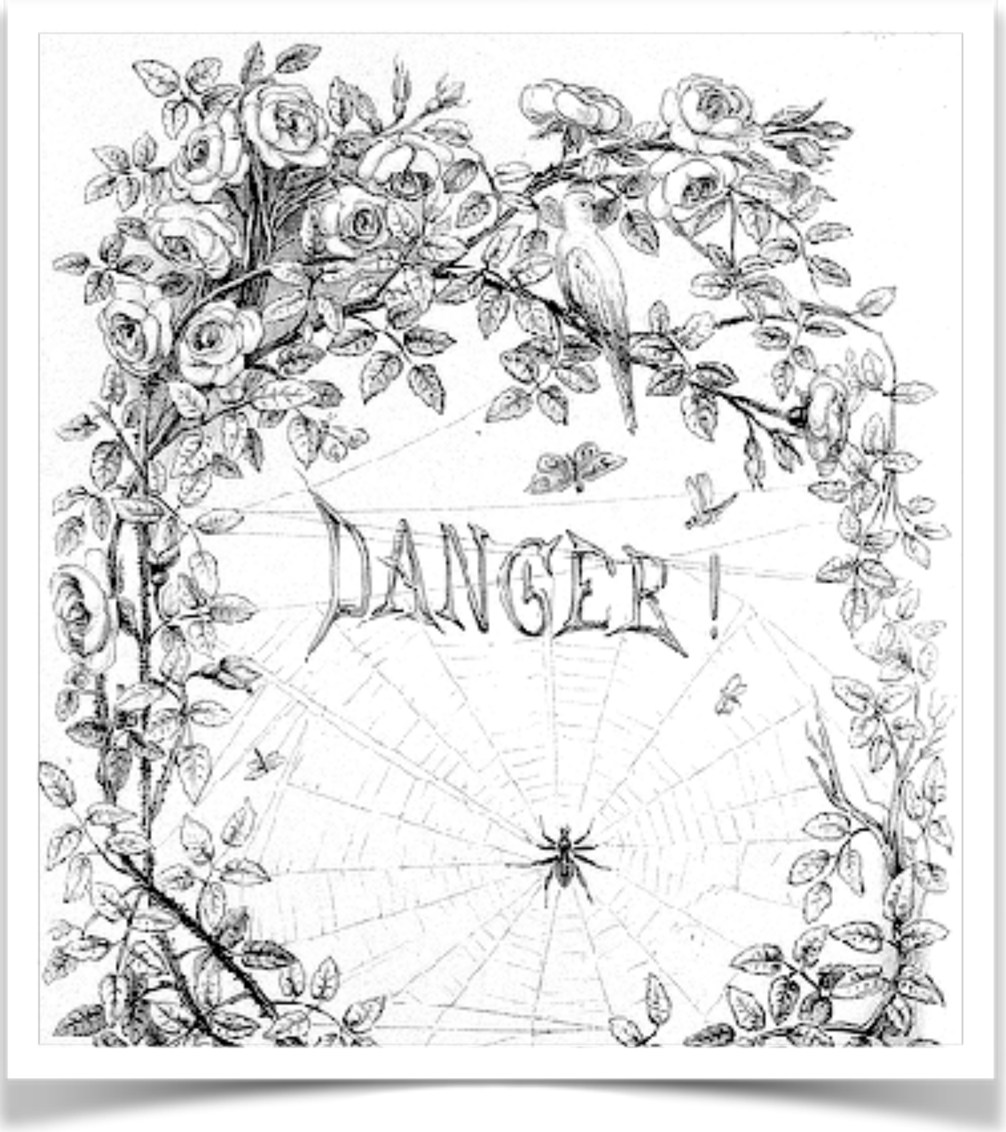


Quantifying Risk

Tie rewards to impact based on a reasonable threat model that reduces subjectivity.

More art than science.

Aim for consistency.



$0-$15K

~$800 avg.

Bounty Variance — XSS

Reflected against self

"Click this link"

Public documentation

$50

https://entire.internet

Authenticated sessions

No user interaction

Affects sensitive content

$10,000

https://klikki.fi/adv/yahoo.html

Bug Value

Well-written descriptions and reproduction steps (that could also be rewarded in price).

Finding (unexploited?) flaws in production code that creates a feedback loop for the SDL.

…and generate tests to catch regression.

…and refactoring code.

…and deploy mitigating controls.

Bug Fixes

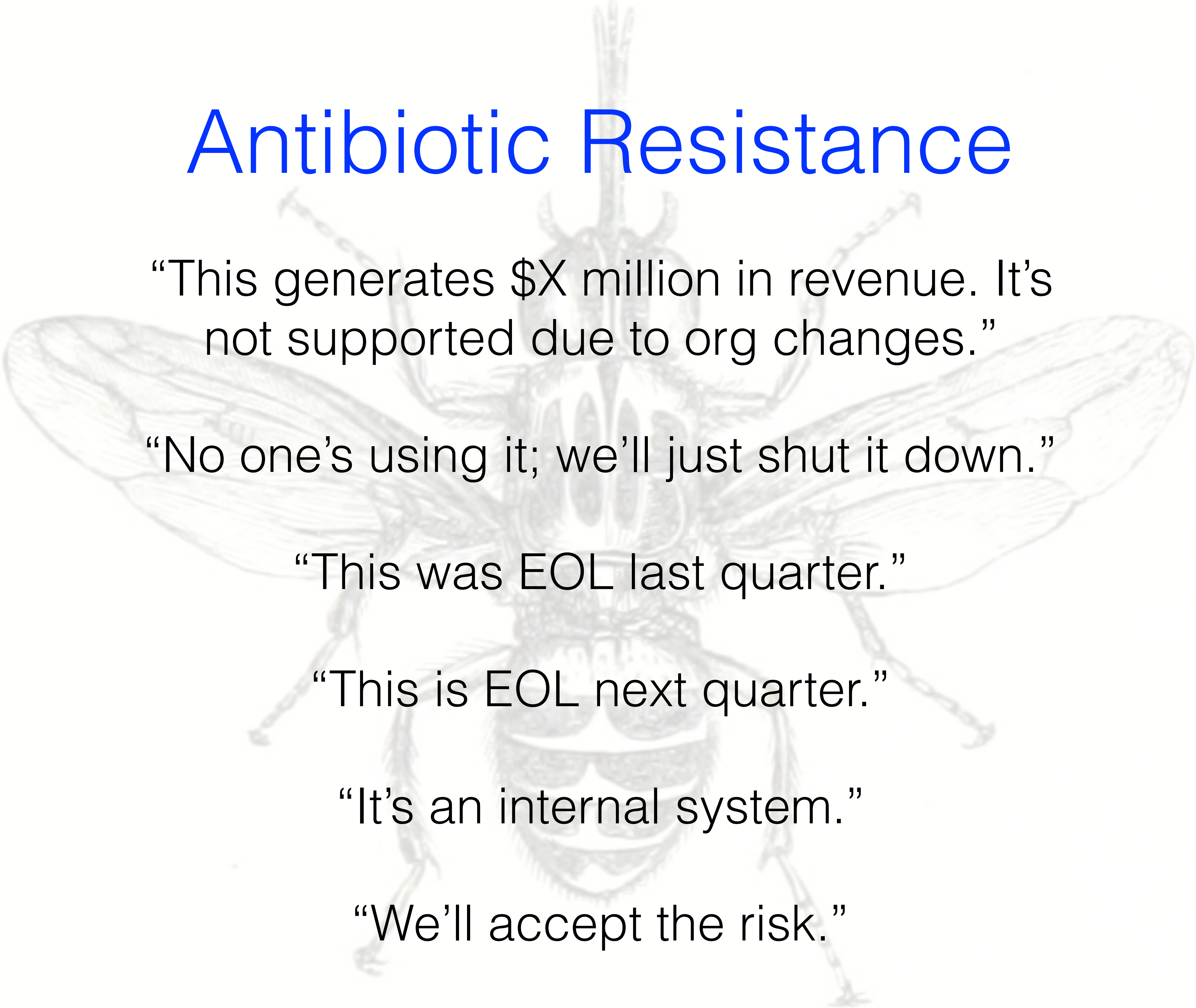
Check in code, deploy a new package, remove old package.

Make sure all systems receive the new code.

Watch for recidivism due to inadequate resolution.

Same bug __ months later

Antibiotic Resistance



“This generates $X million in revenue. It’s not supported due to org changes.”

“No one’s using it; we’ll just shut it down.”

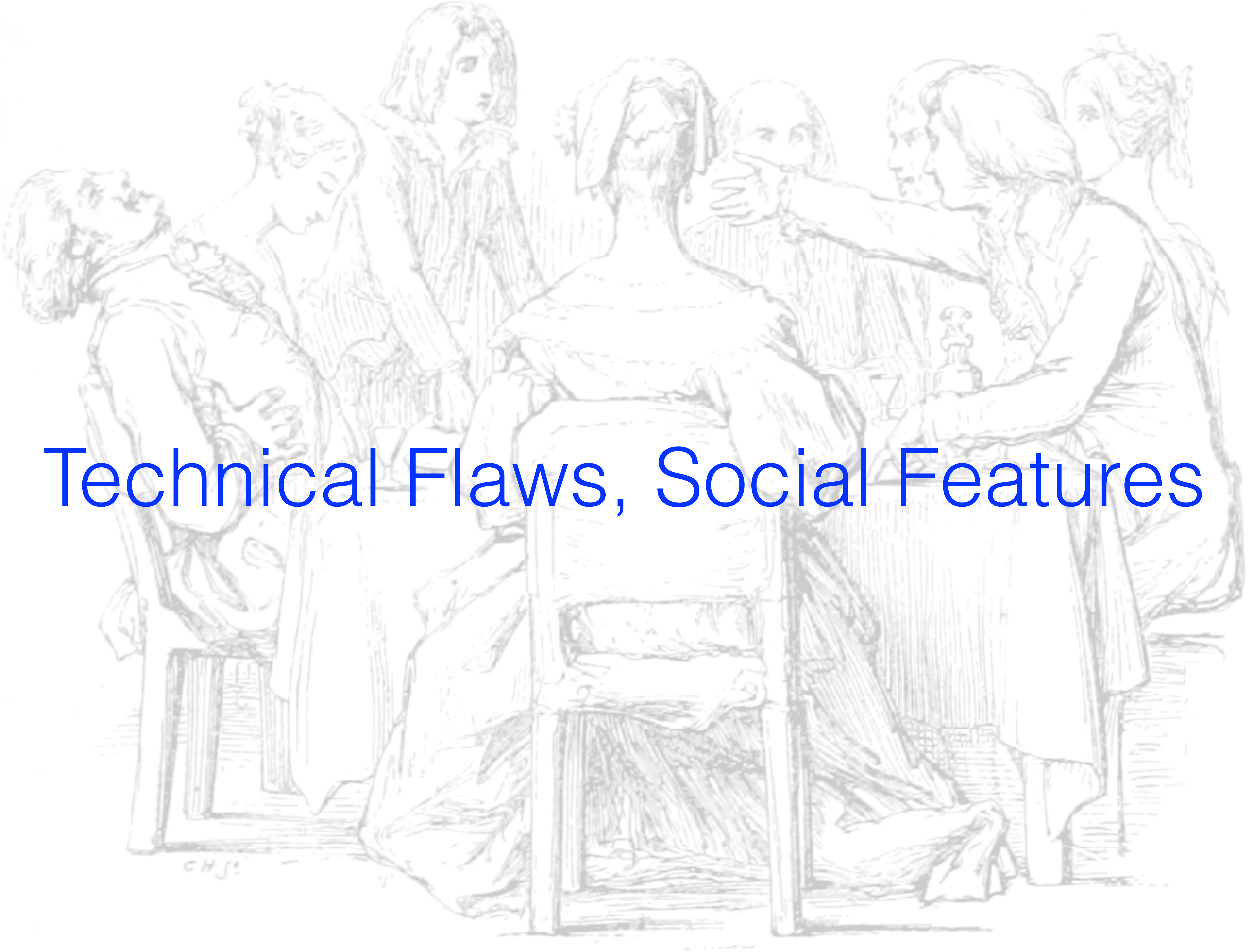
“This was EOL last quarter.”

“This is EOL next quarter.”

“It’s an internal system.”

“We’ll accept the risk.”

Technical Flaws, Social Features



Flexibility, Transparency

Expect to changes rules.

Expect to change scope.

Be clear, address ambiguity.

Be wary, avoid over-analyzing.

Document and track everything.

Adaptation

Communication

Working with researchers

Invite, reward

Warn, ban

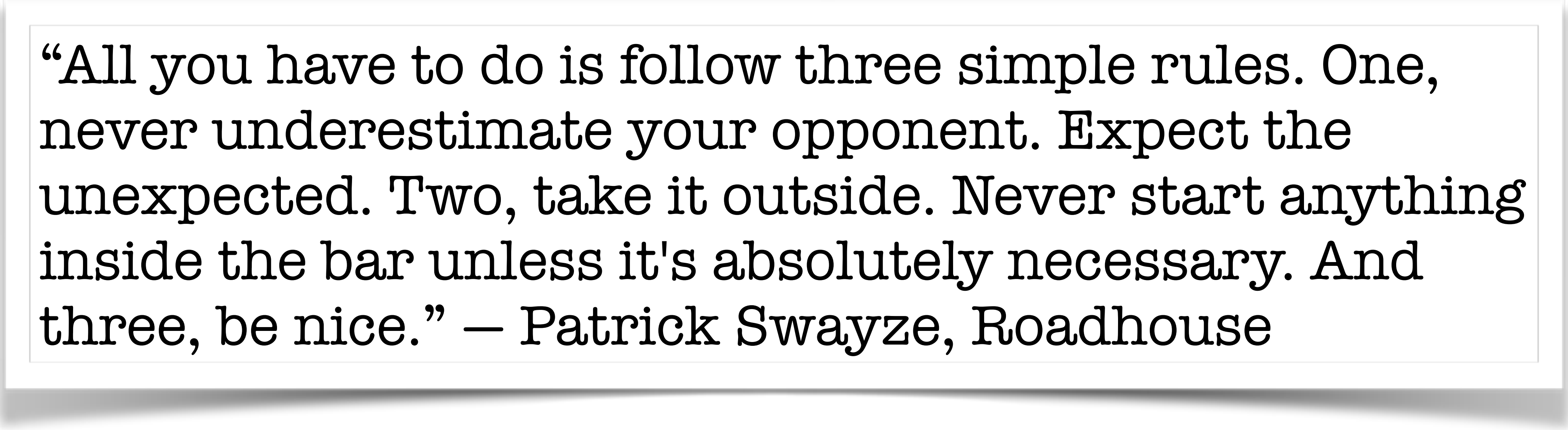
Preparing for fallout

Working with devs

Explaining vulns

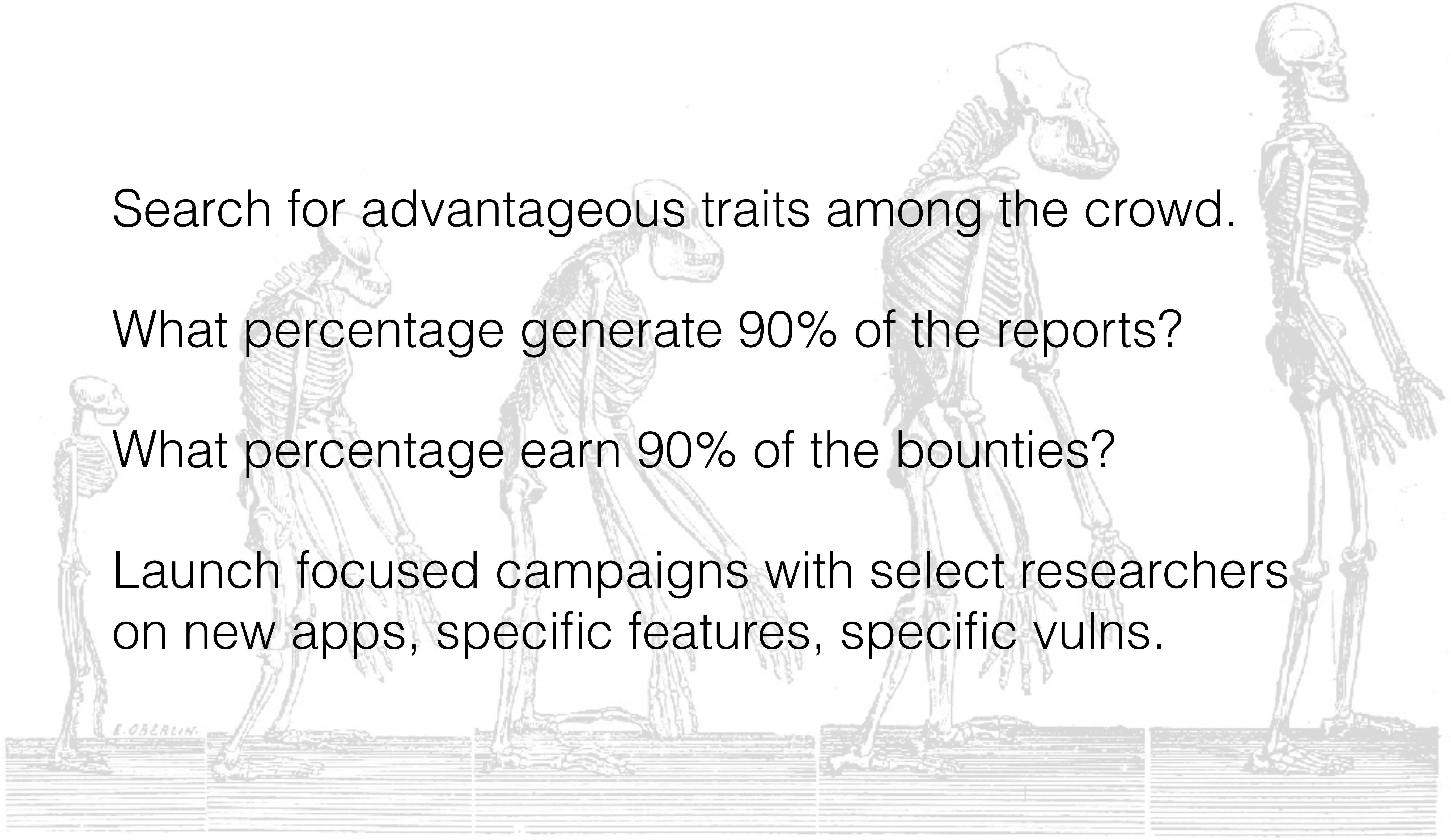
Negotiating priority

Measuring progress



"All you have to do is follow three simple rules. One, never underestimate your opponent. Expect the unexpected. Two, take it outside. Never start anything inside the bar unless it's absolutely necessary. And three, be nice." — Patrick Swayze, Roadhouse

Natural Selection



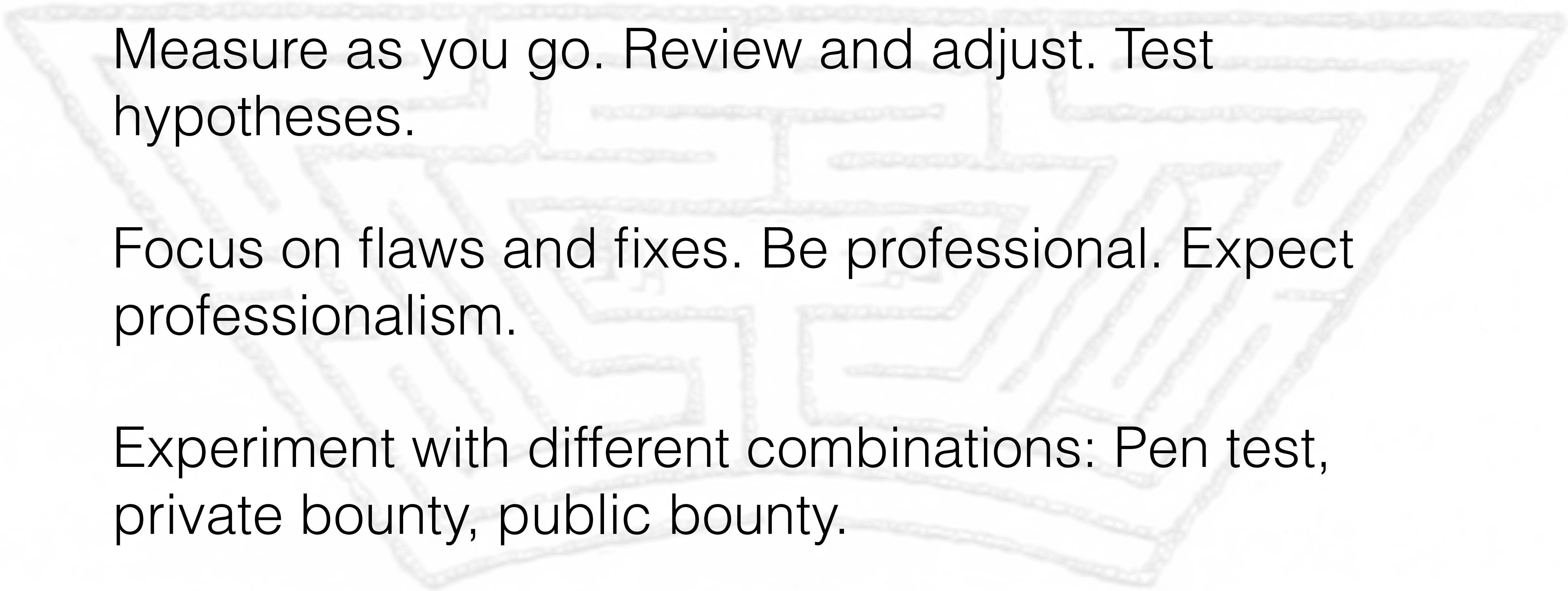
Search for advantageous traits among the crowd.

What percentage generate 90% of the reports?

What percentage earn 90% of the bounties?

Launch focused campaigns with select researchers on new apps, specific features, specific vulns.

Navigating the Swarm

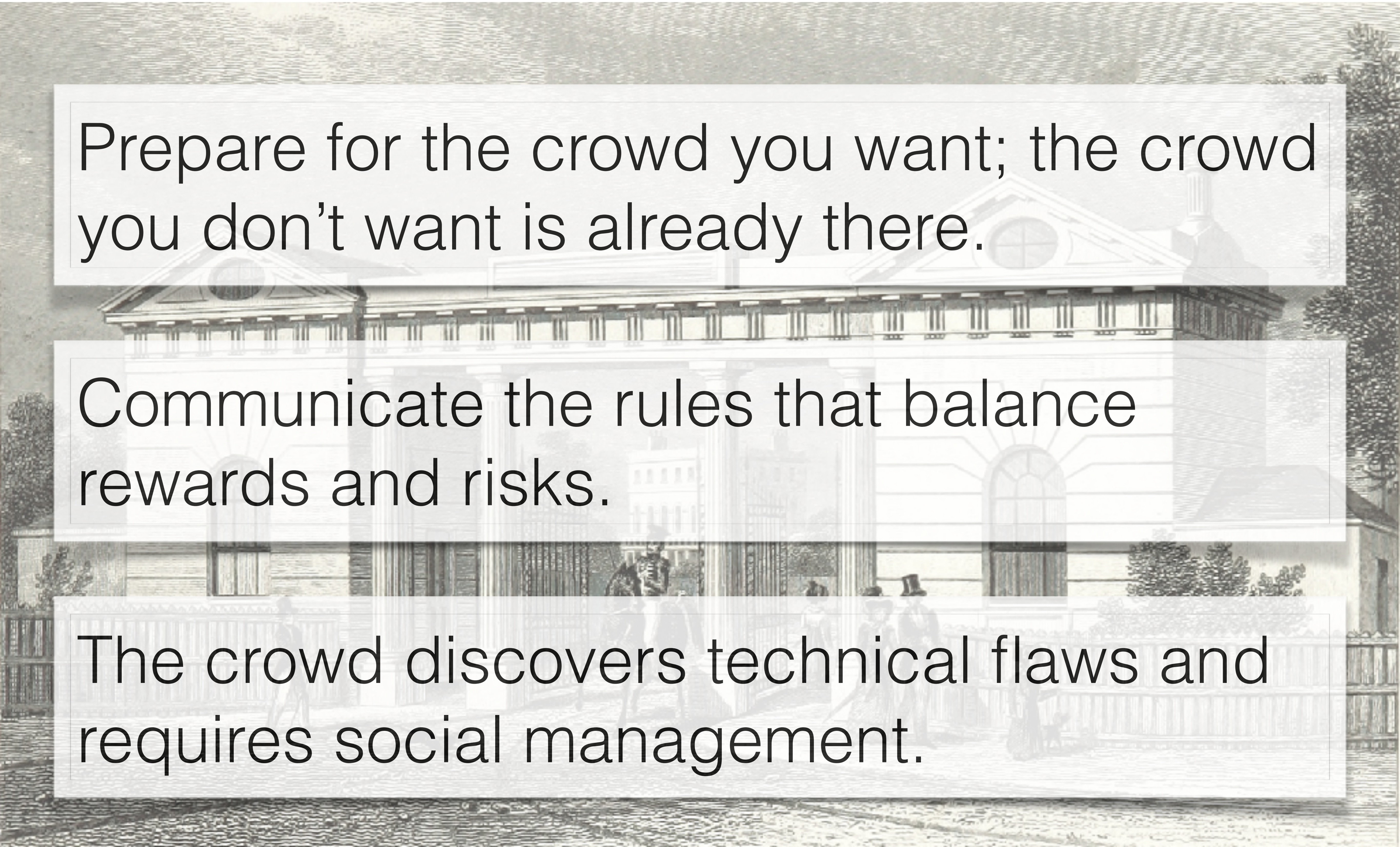


Measure as you go. Review and adjust. Test hypotheses.

Focus on flaws and fixes. Be professional. Expect professionalism.

Experiment with different combinations: Pen test, private bounty, public bounty.

Before You Leave



Prepare for the crowd you want; the crowd you don't want is already there.

Communicate the rules that balance rewards and risks.

The crowd discovers technical flaws and requires social management.

Thank You!

mike@cobalt.io
https://deadliestwebattacks.com

References

https://www.facebook.com/notes/facebook-bug-bounty/facebook-bug-bounty-5-million-paid-in-5-years/1419385021409053

https://www.facebook.com/notes/facebook-security/an-update-on-our-bug-bounty-program/10151508163265766/

https://yahoo-security.tumblr.com/post/146014375610/not-all-bugs-are-created-equal

https://blog.twitter.com/2016/bug-bounty-2-years-in

https://www.netmeister.org/blog/bug-bounty.html

The British Library released public domain images for anyone to use, remix, and repurpose. Have fun!

http://britishlibrary.typepad.co.uk/digital-scholarship/2013/12/a-million-first-steps.html

https://www.flickr.com/people/britishlibrary/