RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: HT-R04F

…But Now I See - a Vulnerability Disclosure Maturity Model

hackerone

Who the FSCK Are You? What is it you do here?

Chief Policy Officer, HackerOne

Former Microsoft Security Strategist

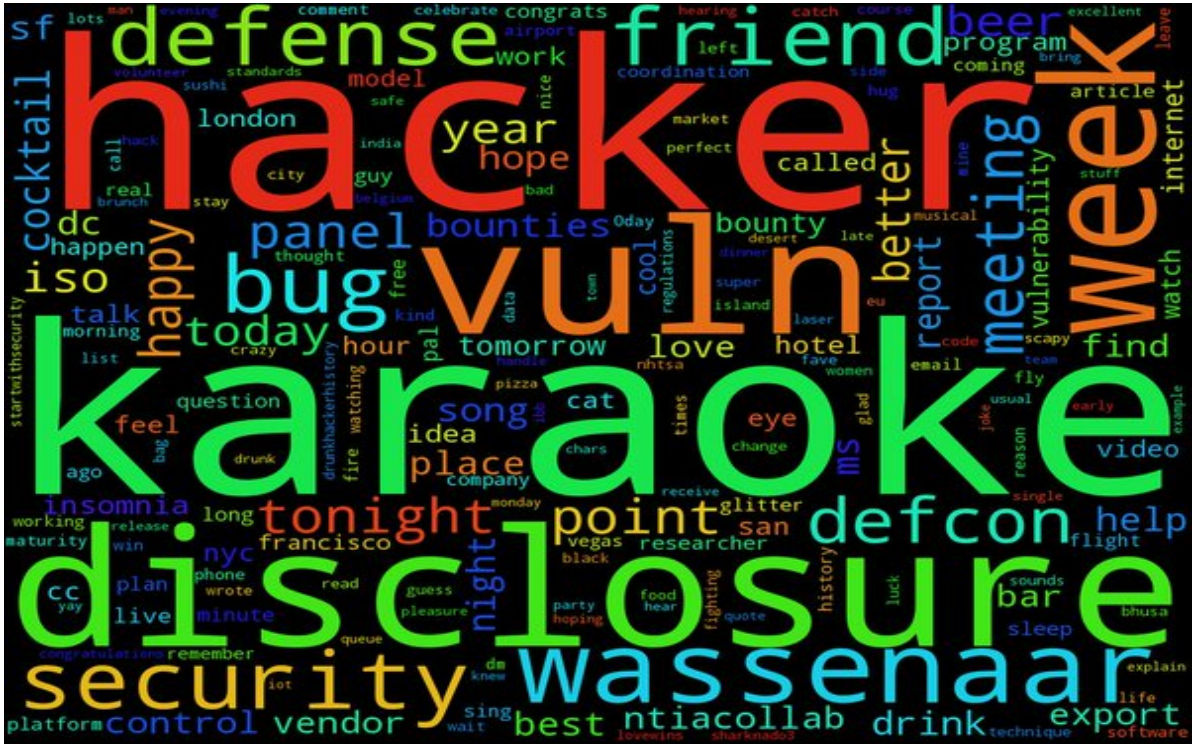
Former Hacker for Hire

ISO Standards Editor

New America Foundation Fellow

MIT Sloan Visiting Scholar

Harvard Belfer Affiliate



hackerone

Measuring Our Maturity

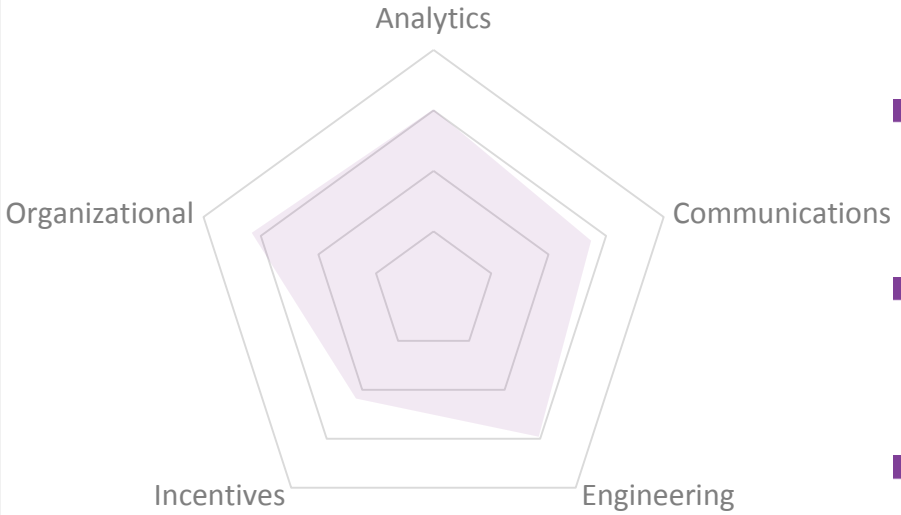
- How would you answer these questions?
  - When someone emails security@mycompany, who responds? How quickly?
  - Would my company's legal department threaten a well-intentioned hacker who came to us with a valuable bug?

Measuring Our Maturity

- Does engineering prioritize the importance of product features alongside security bugs that come in from the wild?
- If a reporter asked my CEO about a breach reported at our company, would she know what steps were taken to ensure user safety?
- Is $10,000 is too much, too little, or just right to offer a hacker for a bug?

The 5 Key Elements of Vulnerability Coordination Maturity

Vulnerability Coordination Maturity Model



- New model for organizations to assess maturity of their vulnerability coordination process
- Model guides how to organize and improve efforts inside and outside of an organization
- 5 Capability Areas: Organizational, Engineering, Communications, Analytics and Incentives
- 3 Maturity Levels for each Capability: Basic, Advanced or Expert
- Companies can benchmark their capabilities against the industry

Organizational

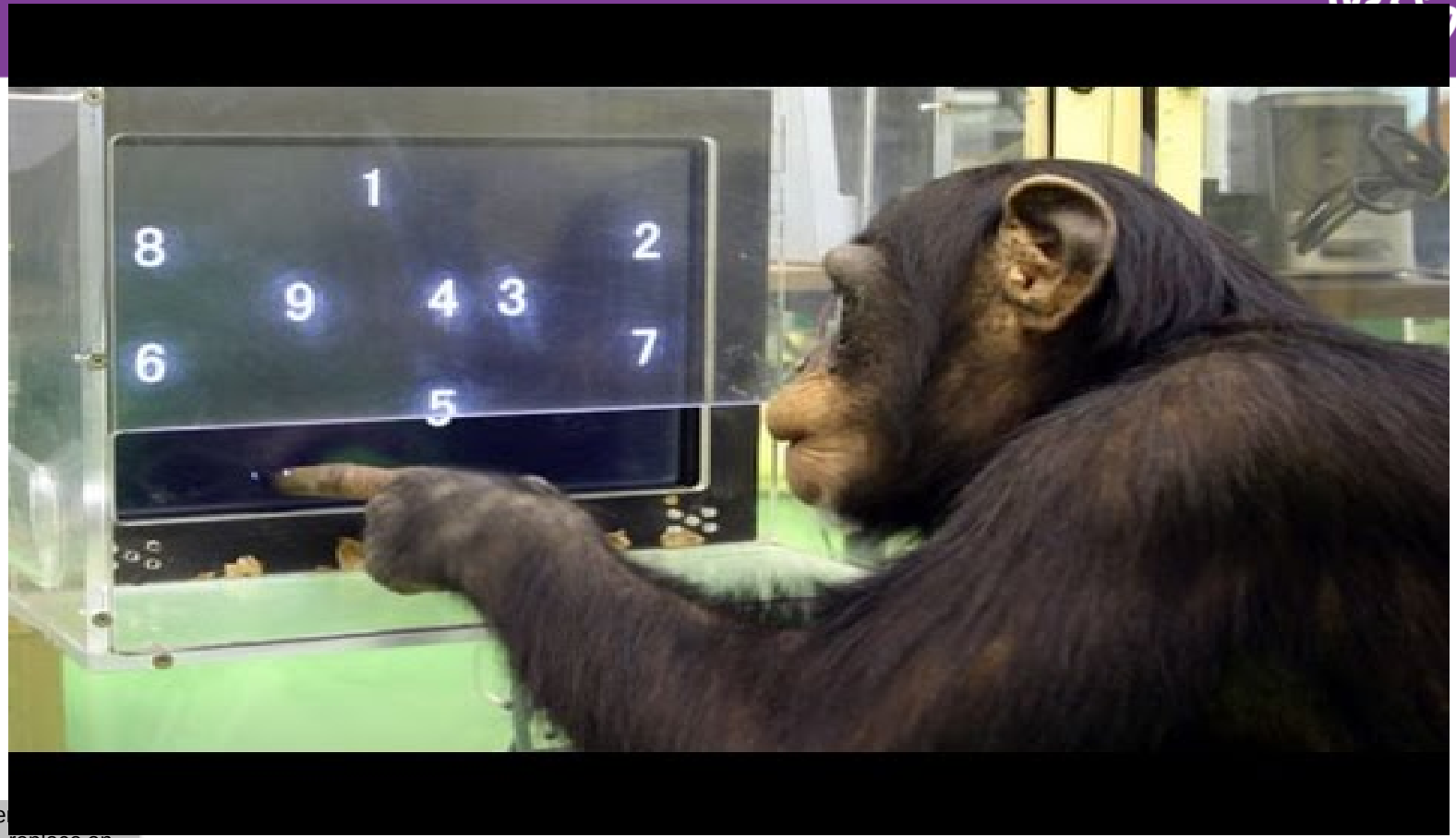
People, process, and resources to handle potential vulnerabilities

Level	Capability
Basic	Executive support to respond to vulnerability reports and a commitment to security and quality as core organizational values.
Advanced	Policy and process for addressing vulnerabilities according to ISO 29147 and ISO 30111, or a comparable framework.
Expert	You have executive support, processes, budget and dedicated personnel for handling vulnerability reports.

Engineering

Capabilities to evaluate and remediate security holes, and improve software development lifecycle

Level	Capability
Basic	Clear way to receive vulnerability reports, and an internal bug database to track them to resolution. See ISO 29147.
Advanced	Dedicated security bug tracking and documentation of security decisions, deferrals, and trade-offs.
Expert	Use vulnerability trends and root cause analysis to eliminate entire classes of vulnerabilities. See ISOs 29147, 30111, 27034.



Presenter Logo – replace on master slide

Communications

Ability to communicate to audiences internally and externally about vulnerabilities.

Level	Capability
Basic	Ability to receive vulnerability reports and a verifiable channel to distribute advisories to affected parties. See ISO 29147.
Advanced	Tailored, repeatable communications for each audience, including security researchers, partners, customers, and media.
Expert	Structured information sharing programs with coordinated distribution of remediation.

Presentation Logo – replace on master slide

Analytics

Data analysis of vulnerabilities to identify trends and improve processes.

Level	Capability
Basic	Track the number and severity of vulnerabilities over time to measure improvements in code quality.
Advanced	Use root causes analysis to feed back into your software development lifecycle. See ISOs 29147, 30111, 27034.
Expert	Track real-time telemetry of active exploitation to drive dynamic pivots of remediation strategy.

Logo – replace on master slide

Incentives

Ability to encourage security researchers to report vulnerabilities directly.

Level	Capability
Basic	Show thanks or give swag. Clearly state that no legal action will be taken against researchers who report bugs.
Advanced	Give financial rewards or bug bounties to encourage reporting the most serious vulnerabilities.
Expert	Understand adversary behavior and vulnerability markets, and structure advanced incentives to disrupt them.


hacker

Measuring Success in Vulnerability Disclosure

A look at 100+ Companies

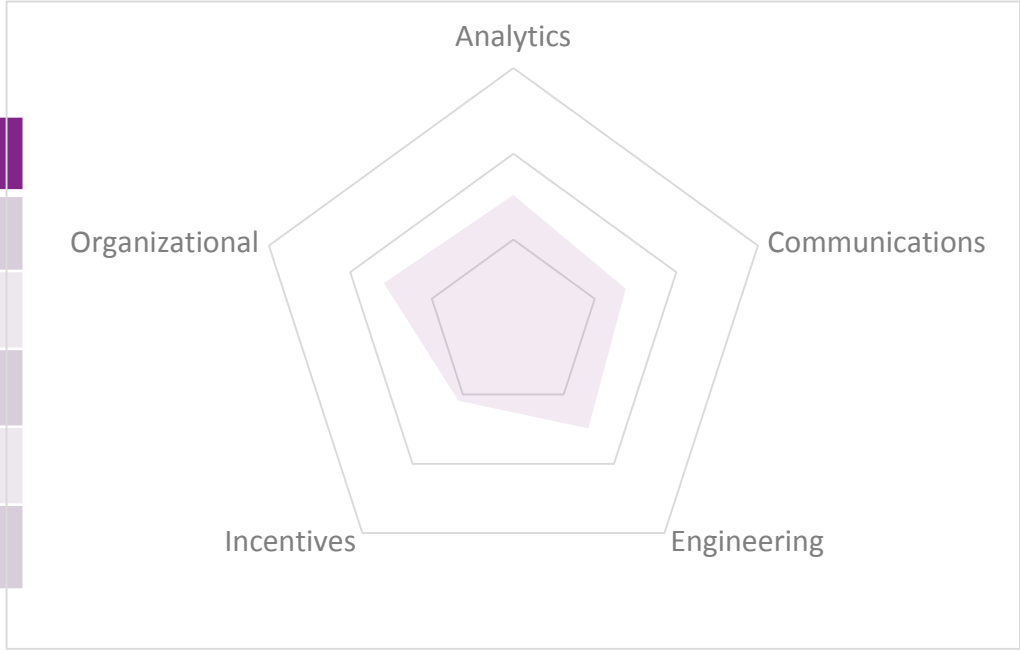
Measuring Success in Vulnerability Disclosure

Survey Data

N=194
IT/Security Professionals
Collected between Sept. 2015 – Jan. 2016 via online survey

Measuring Success in Vulnerability Disclosure

Capability	Mean Score
Analytics	1.52
Communications	1.38
Engineering	1.49
Incentives	1.09
Organizational	1.59



Avg. By Industry (min. 10 respondents)

Industry	Sample Size	Analytics	Communications	Engineering	Incentives	Organizational
Education	15	1.27	1.27	1.40	0.67	1.53
Finance	15	2.07	1.47	**2.20**	1.53	2.00
Government	10	1.50	1.20	1.20	**0.40**	1.60
Healthcare	13	1.54	1.46	1.54	0.92	1.54
Manufacturing	21	1.52	1.52	1.62	1.14	1.67
Other	15	1.13	1.20	1.00	0.93	1.73
Technology - B2B	37	1.62	1.49	1.54	1.30	1.70
Technology - B2C	17	1.24	1.18	1.24	1.06	1.24
Technology - Mobile Apps	10	1.90	**1.90**	1.90	1.60	2.10
Unknown	10	1.40	1.50	1.30	1.00	1.40
	163	**1.52**	**1.42**	**1.50**	**1.10**	**1.65**

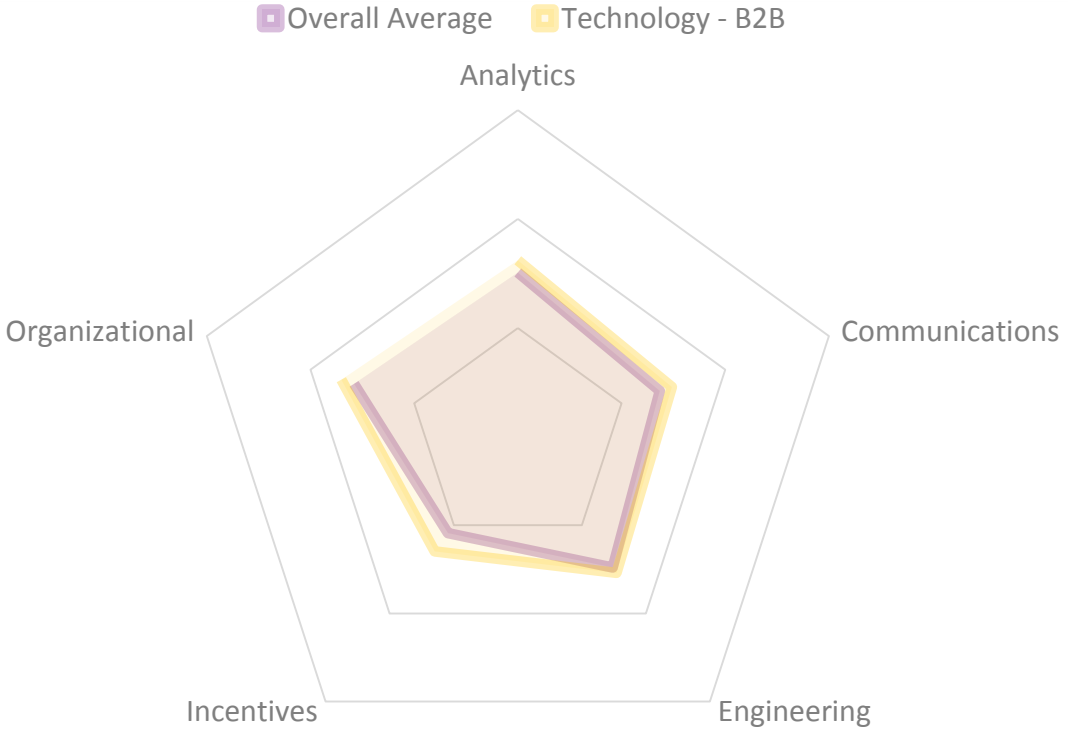
Green = 1 σ above Red = 1 σ below Bold = 2σ above or below

Measuring Success in Vulnerability Disclosure

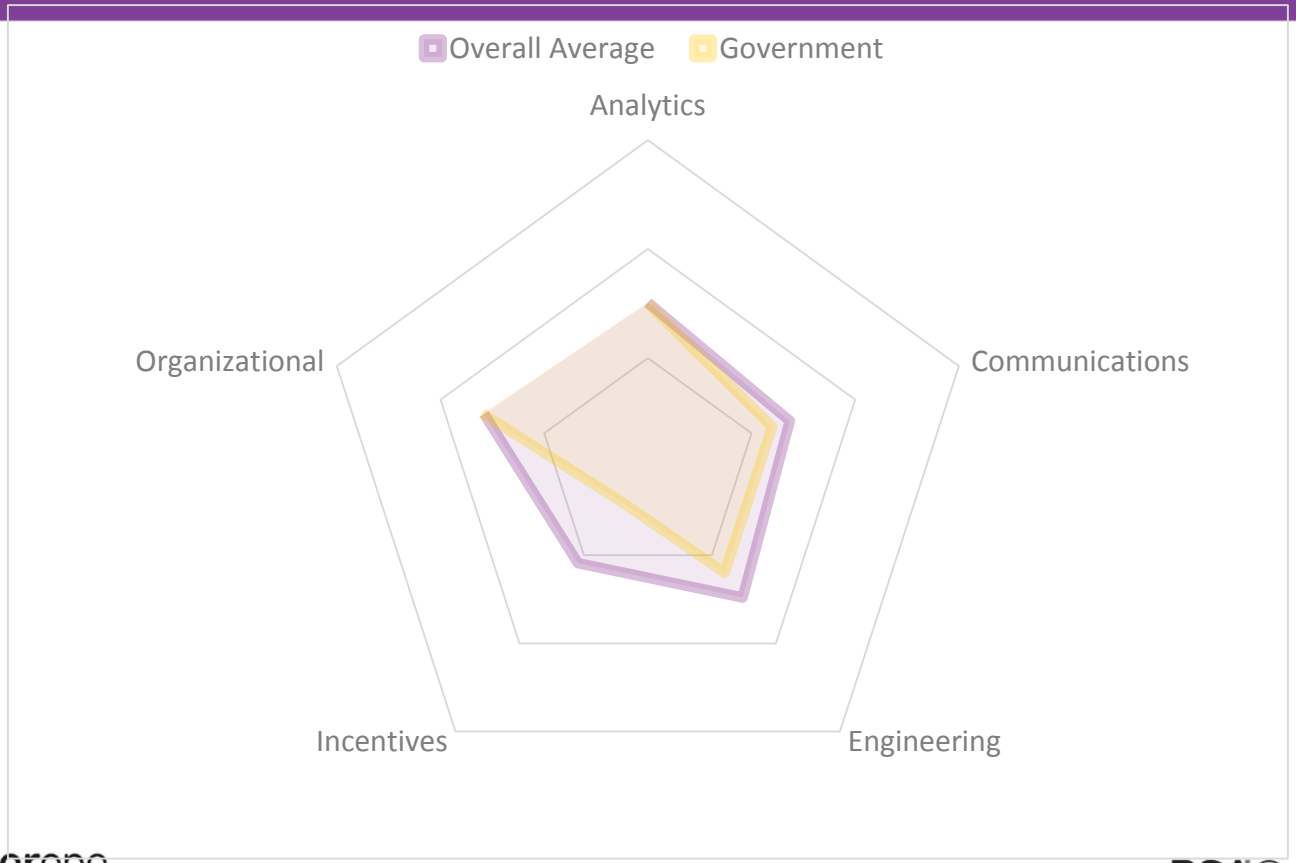
Rank of Industry by Capability, min. 10 respondents (1 = best, 10 = worst)

	Analytics	Comms	Engineering	Incentives	Organizational
Finance	1	5	1	2	2
Technology - Mobile Apps	2	1	2	1	1
Technology - B2B	3	4	4	3	4
Healthcare	4	6	5	8	7
Manufacturing	5	2	3	4	5
Government	6	8	9	10	6
Unknown	7	3	7	6	9
Education	8	7	6	9	8
Technology - B2C	9	10	8	5	10
Other	10	9	10	7	3

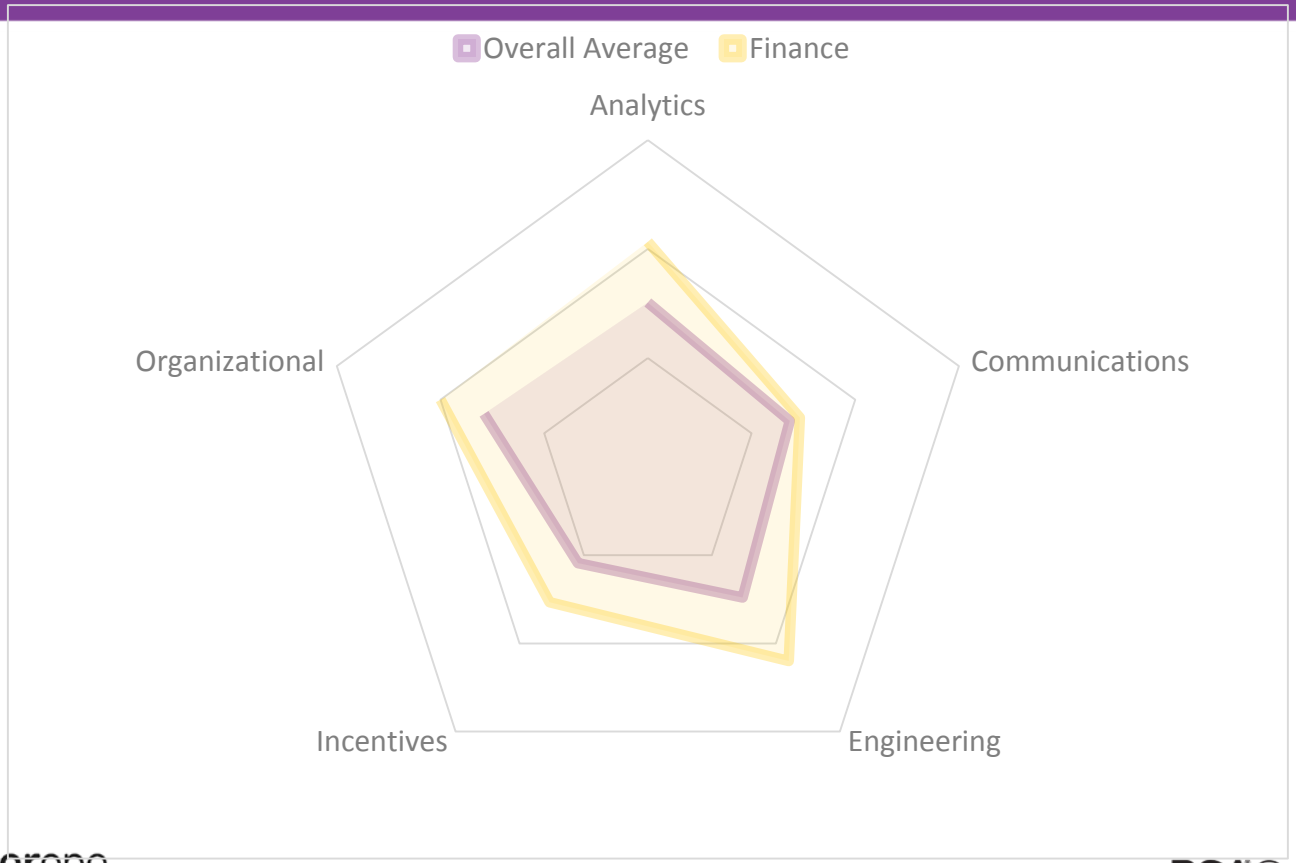
Technology – B2B vs Overall Average



Government vs Overall Average

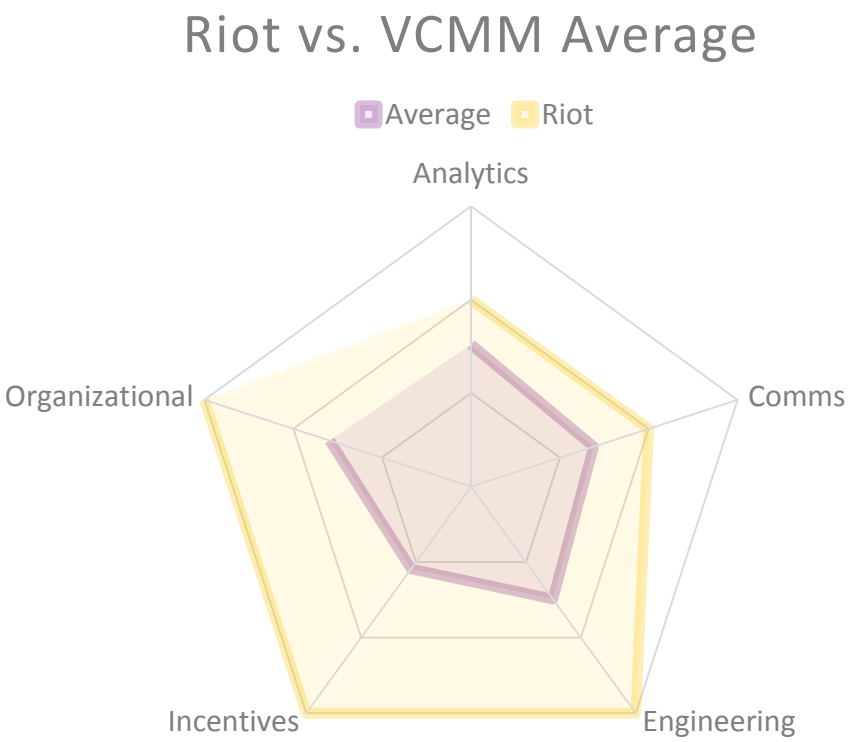


Finance vs Overall Average



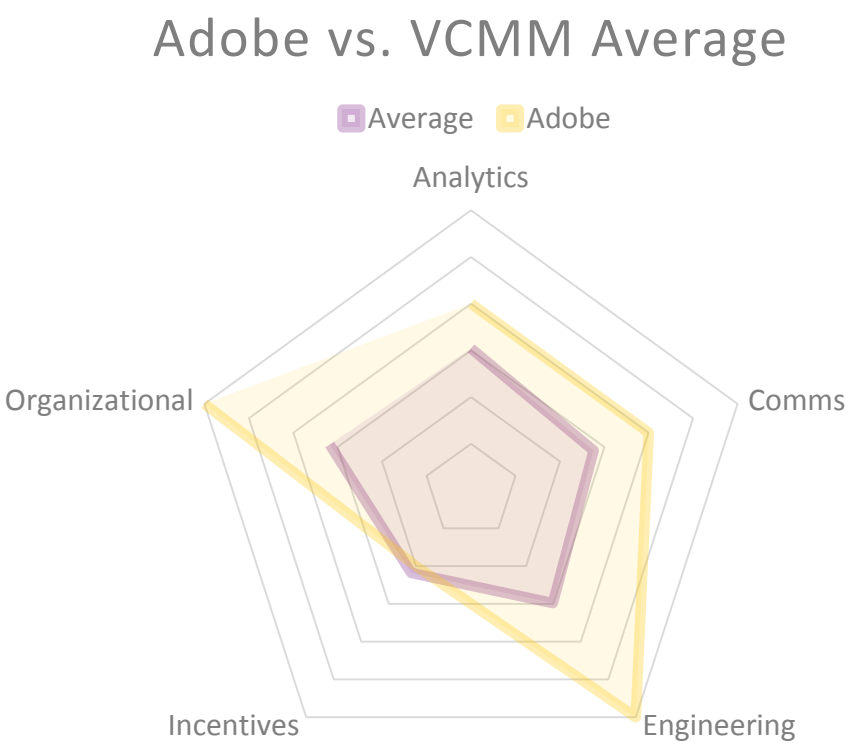
Sample Company – Riot

Capability	Average	Riot
Analytics	1.52	2
Comms	1.38	2
Engineering	1.49	3
Incentives	1.09	3
Org.	1.59	3



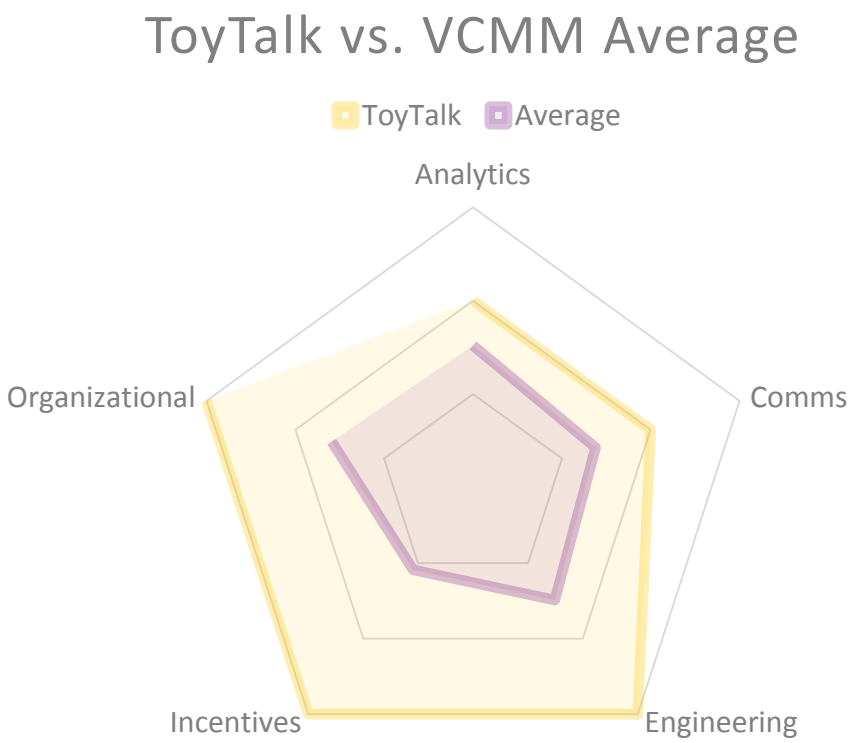
Sample Company – Adobe

Capability	Average	Adobe
Analytics	1.52	2
Comms	1.38	2
Engineering	1.49	3
Incentives	1.09	1
Org.	1.59	3



Sample Company – ToyTalk

Capability	Average	ToyTalk
Analytics	1.52	2
Comms	1.38	2
Engineering	1.49	3
Incentives	1.09	3
Org.	1.59	3



Next Steps

- Continue to gather data
  - Non self-reported
  - Larger sample size
- Multi-vendor coordination is needed

Put Your Organization To The Test – Where Do You Rank

“Apply”

- Take the free maturity assessment within minutes at hackerone.com/vulnerability-coordination-maturity-model

Appendix