MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

FROM HACK THE PENTAGON TO MAINSTREAM:

WHY BUG BOUNTIES ARE NOW IN EVERY SECTOR

Jon Bottarini

Security Researcher

HackerOne

My background

- Hacker!

- Participate in multiple bug bounty programs – even ones I know help managed.

- Technical Program Manager at HackerOne: I help organizations like the US Department of Defense, General Service Administration, Yahoo! (and more!) secure their assets and run their bug bounty programs

Why should I consider bug bounties?

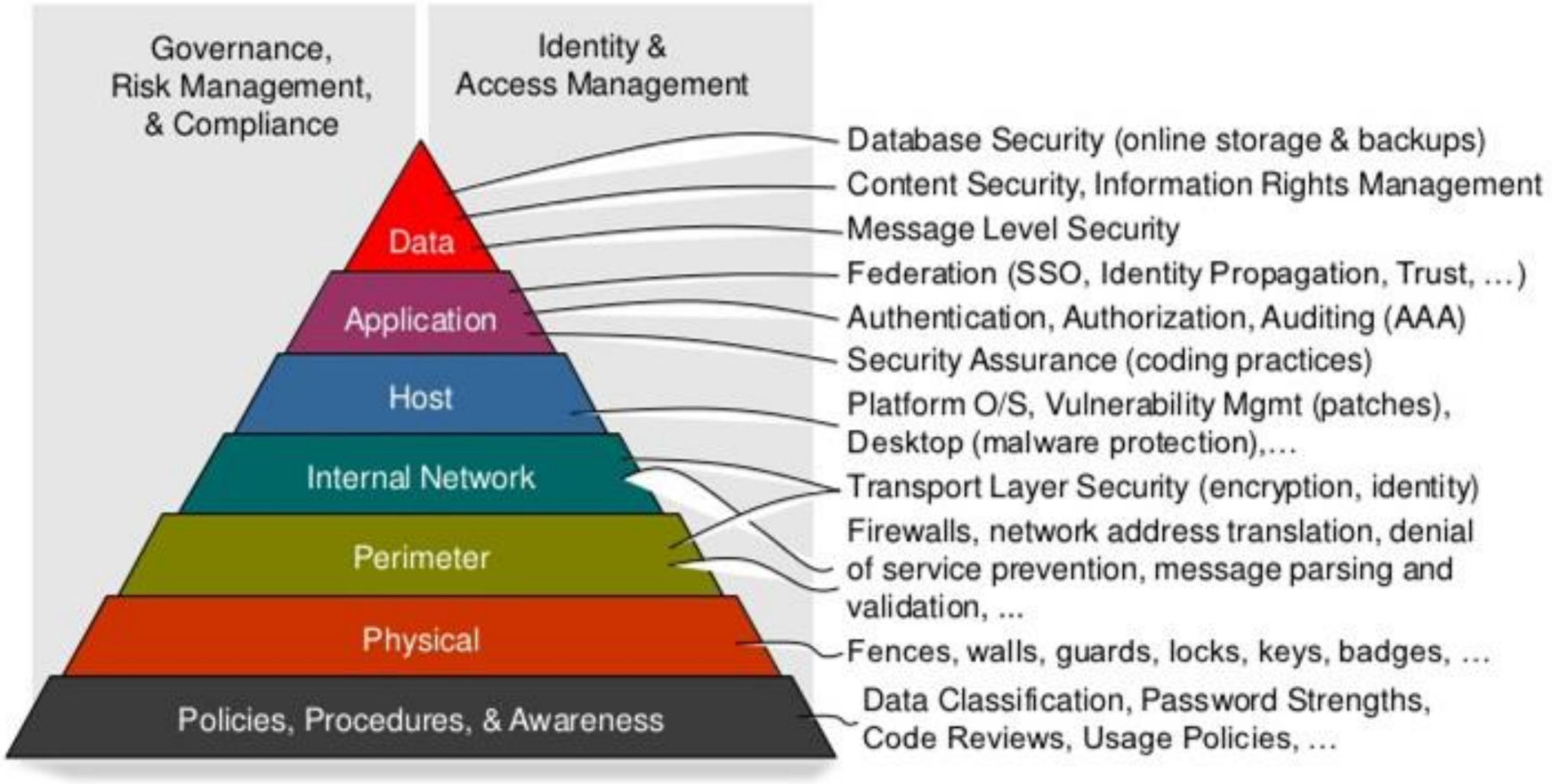


Image credit: https://www.darknet.org.uk/2016/03/defence-depth-web-applications/

- Lots of layers… lots of opportunities for something to go wrong!
- Let’s see if your defense in depth is actually effective!

What can bug bounties do for me?

Where do bug bounties fit in?

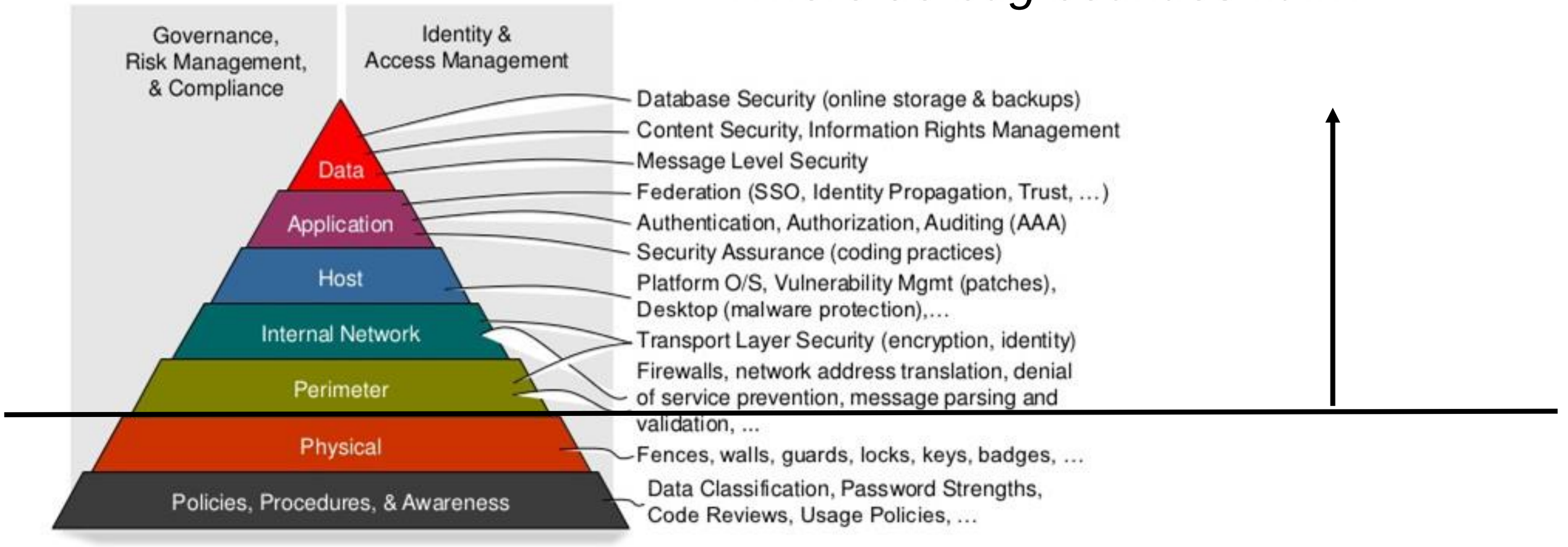


Image credit: https://www.darknet.org.uk/2016/03/defence-depth-web-applications/

Common Misconceptions

We do regular pentests!

Everytime a code change is made? Every feature that is launched? Across all your subdomains?

We have a WAF!

Let me tell you a story…

Storytime…

Common Misconceptions

We do regular pentests!

Everytime a code change is made? Every feature that is launched? Across all your subdomains?

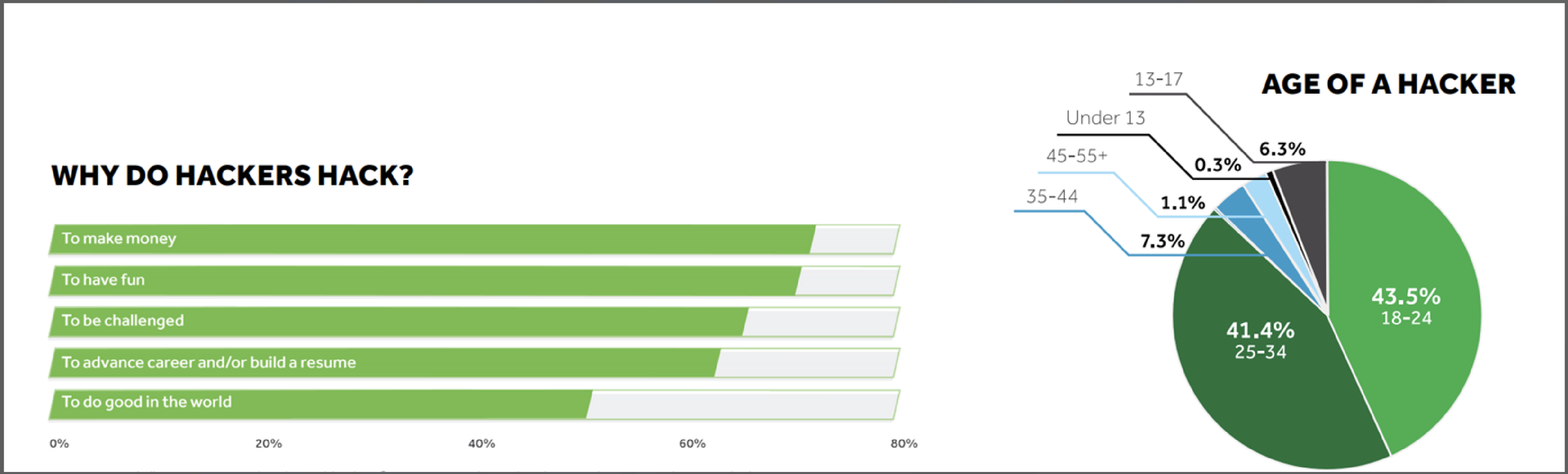
We have a WAF!

Let me tell you a story…

We don’t know who these “hackers” are! What if they break something?

Who are these bug bounty hunters? Why would we let them hack us?

The bad guys are already attacking your systems. Why shouldn't you let the good guys



InfoSecWorld
Conference & Expo 2018

The most horrifying slide you will see all day

The most horrifying slide you will see all day

Even if someone finds a security vulnerability, 94% of the Forbes Global 2000 have NO MEANS to receive the vulnerability.

Source: https://www.hackerone.com/sites/default/files/2017-06/The%20Hacker-Powered%20Security%20Report.pdf

Enter: The US Department of Defense

“My first thought was, ‘Wow, it only took them 10 minutes to identify a vulnerability. How long would it have taken for us to discover?”

- Paul Nakasone, Lieutenant General, Army Cyber Command

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Jon Bottarini

Security Researcher

HackerOne