PCI:
Compromising Controls and Compromising Security

PCI? At DefCon?

Compliance is changing the way companies "do security", and that has an effect on everyone, hacker, defender, attacker, and innocent bystander.

One result is that companies fear QSAs more than 0-days.

Who are we?

- James Arlen, aka Myrcurial
- Anton Chuvakin
- Joshua Corman
- Jack Daniel
- Alex Hutton
- Martin McKeay
- Dave Shackleford

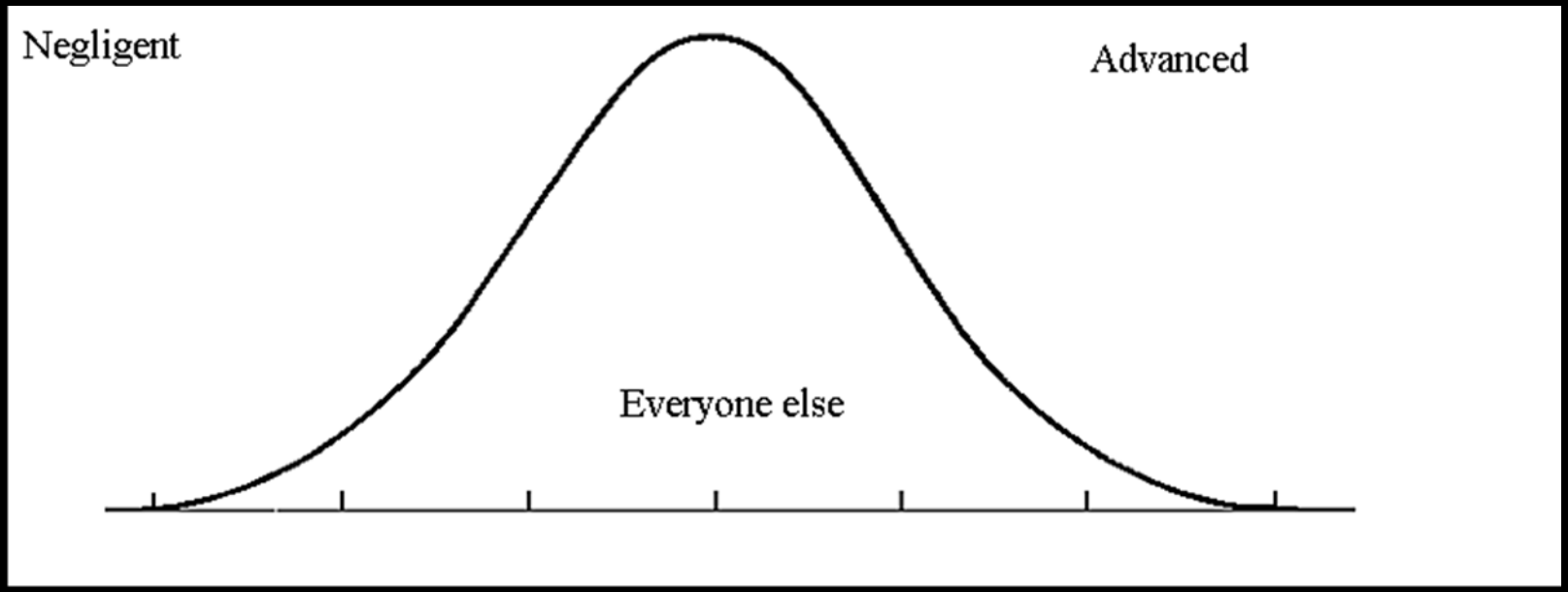
Usual disclaimers

- We do not speak for our employers, clients or customers. Nor for our spouses, siblings, or offspring. But my dog will back me up.
- Our opinions are our own, the facts are as we see them.
- We aren’t lawyers…etc.
- These QSAs are not your QSAs.

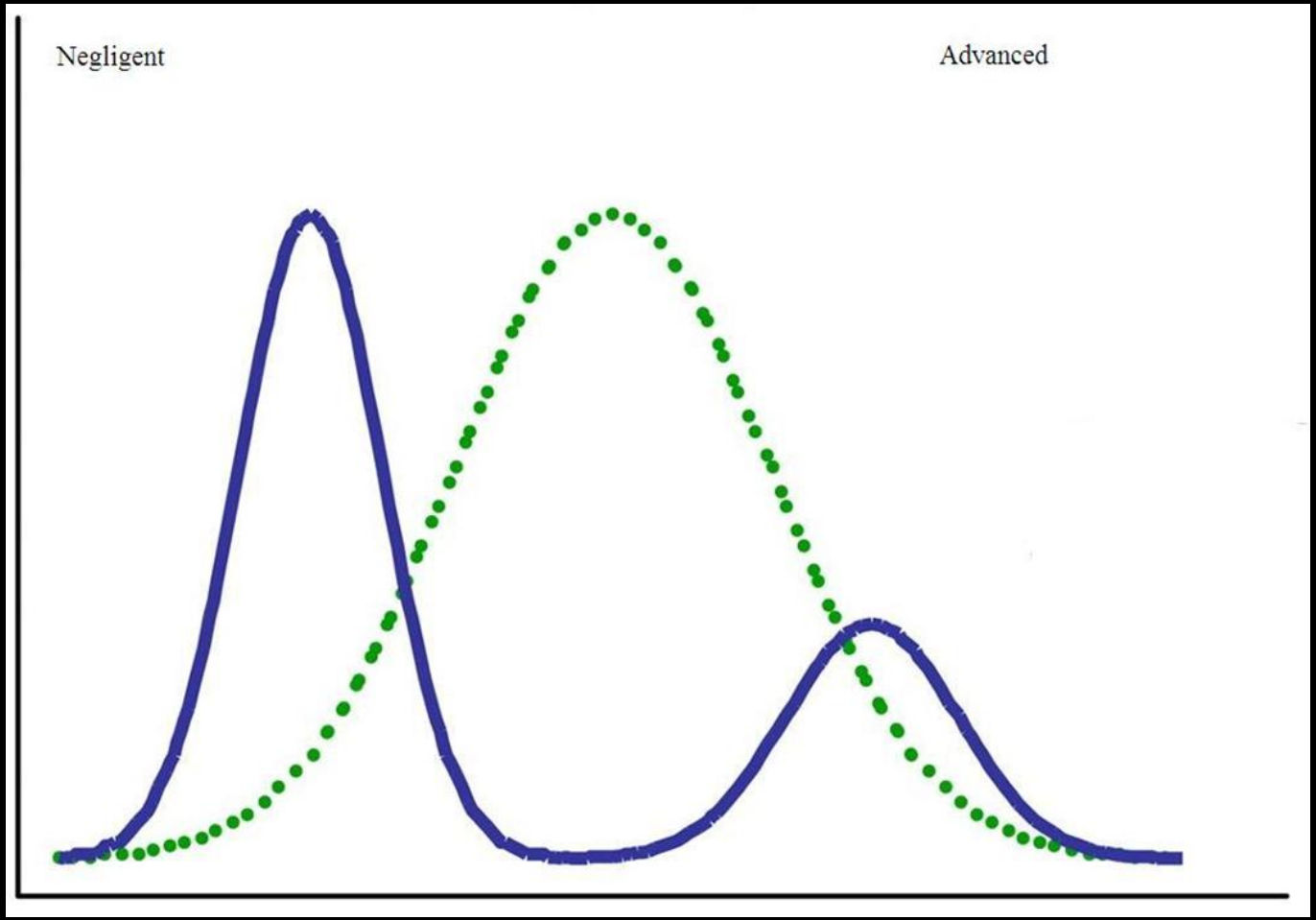
PCI. Discuss.

- PCI vs. Security. Is it really “vs.” security?
- PCI hampers the advanced. Right? Really?
- At least it is timely. And the three years cycle insures that.
- PCI has an impact on ALL of us, even if not under the heel of its hobnail boot. Or does it?

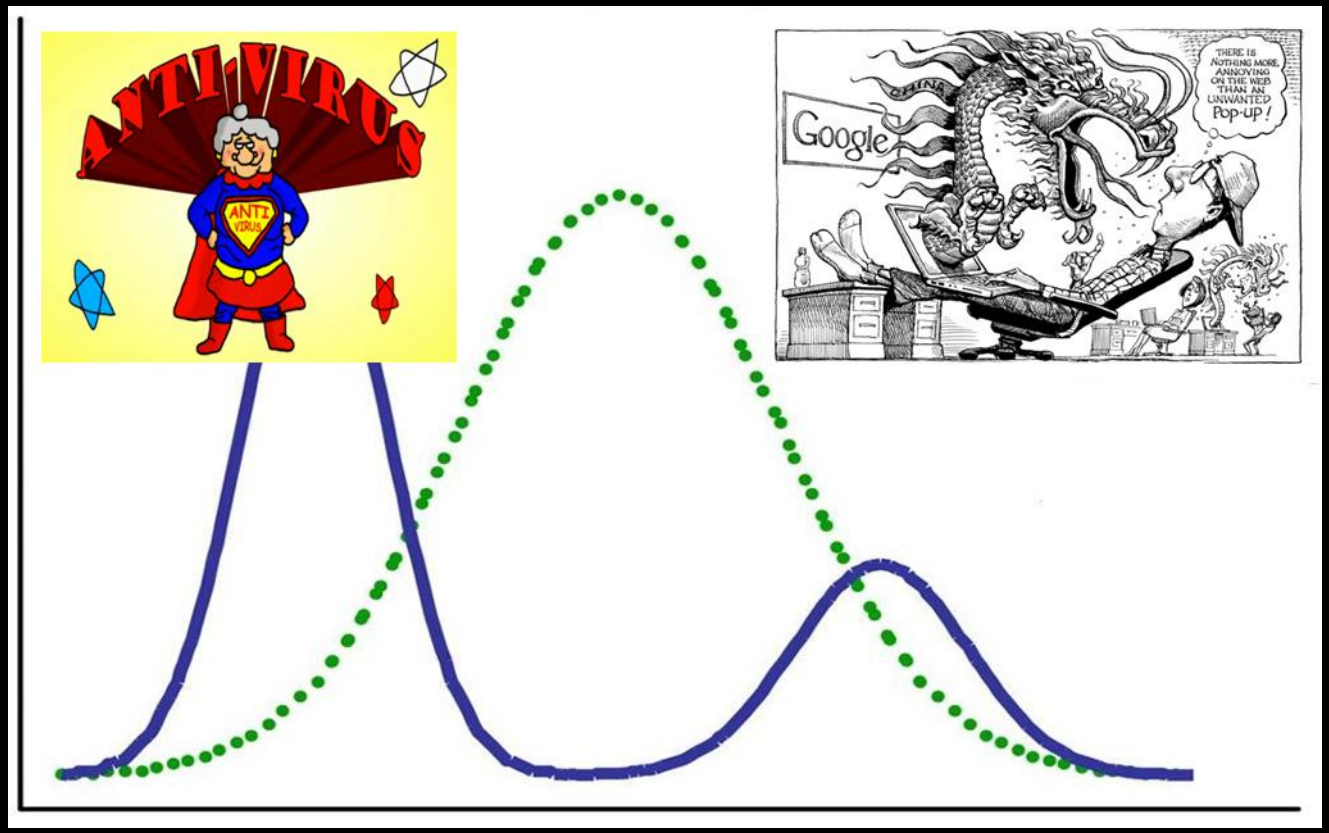
Obligatory Bell Curve Slide



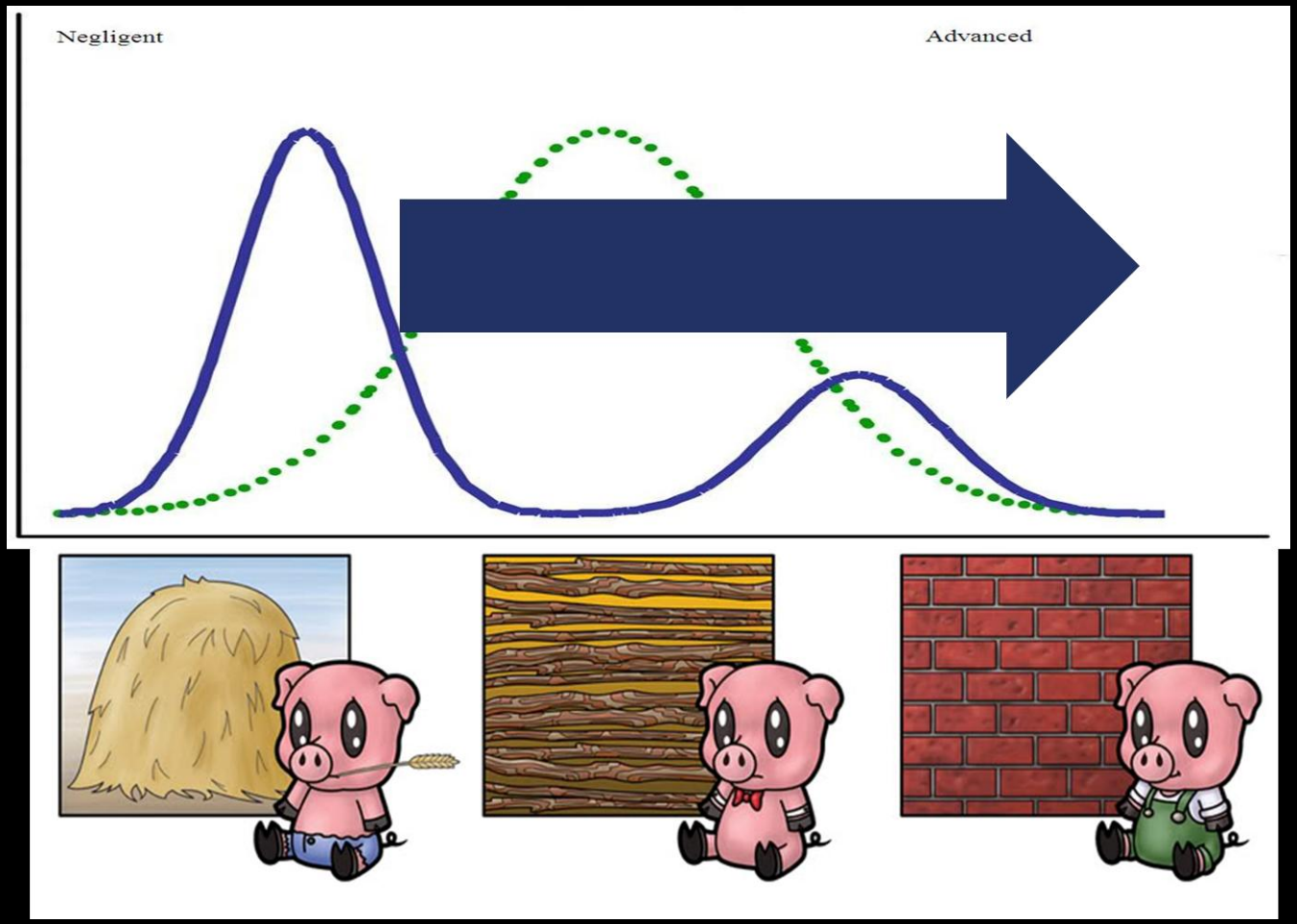
More accurate curves



With pictures, even.



Zombie resistant housing?



PCI and metrics.

- PCI could provide some very useful data about security postures, exposures, breaches, and all kinds of cools stuff.
- Could.
- Does it?
- Should it?

Moving forward

- How do we move forward?
- Who do we have to convince?
- What moves them?

Previous conversations

CSO Online Debate Part 1 of 2:
http://www.csoonline.com/podcast/513988/The_Great_PCI_Security_Debate_of_2010_Part_1

Network Security Podcast Part 2 of 2:
http://netsecpodcast.com/?p=391

Southern Fried Security Podcast – Special Episode:
http://www.southernfriedsecurity.com/episodes-0-9/special-episode---interview-with-josh-corman

ShmooCon 2010
http://www.shmoocon.org/2010/videos/PCI-Panel.flv

BSidesSF Panel Video
http://www.ustream.tv/recorded/5164678 (pt 1)
http://www.ustream.tv/recorded/5165234 (pt 2)

Contact us

- James Arlen @myrcurial
- Anton Chuvakin @anton_chuvakin
- Joshua Corman @joshcorman
- Jack Daniel @jack_daniel
- Alex Hutton @alexhutton
- Martin McKeay @mckeay
- Dave Shackleford @daveshackleford

Thank you

Please continue the conversation, learn, engage, act.

Compliance, and specifically PCI, is poised to steal security from those of us who care about it.