PCI 2.0:
Still
Compromising Controls
and
Compromising Security

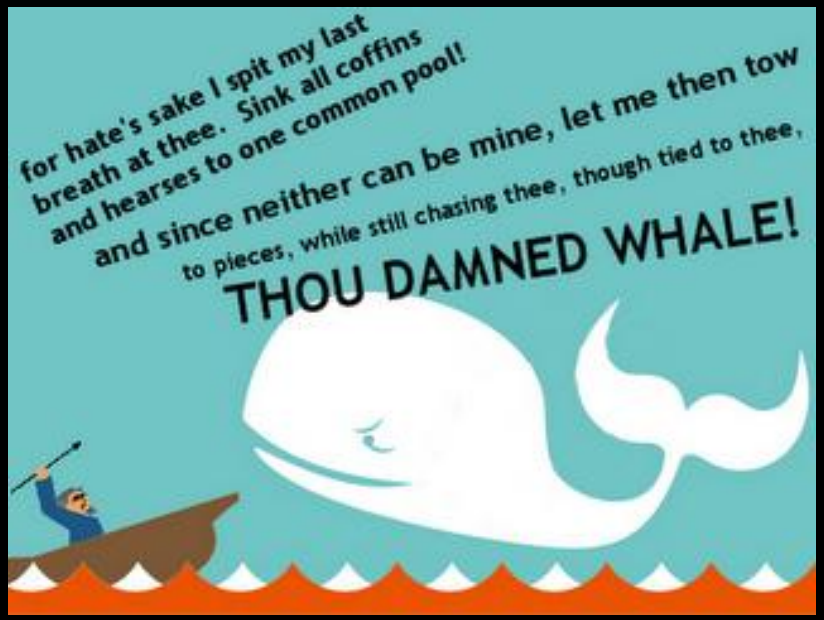
PCI? At DefCon? Again?

Use the hashtag #DefconPCI to rant on the Twitterz during this talk. We damn sure will!

Use @defconPCIpanel for
comments or Twitter-heckling

Who are we?

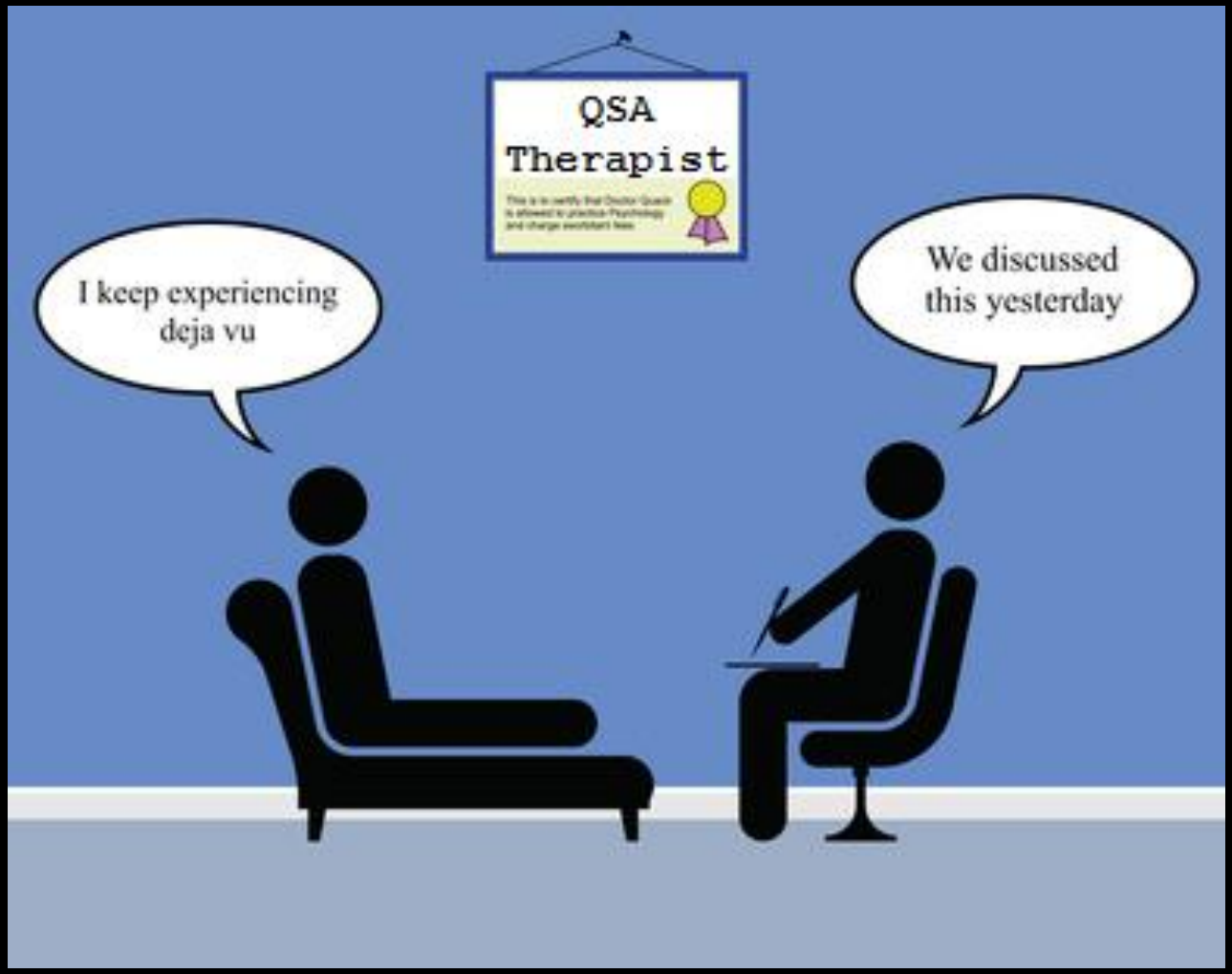
- Dave Shackleford @daveshackleford
- Joshua Corman @joshcorman
- James Arlen @myrcurial
- Jack Daniel @jack_daniel
- Alex Hutton @alexhutton
- Martin McKeay @mckeay



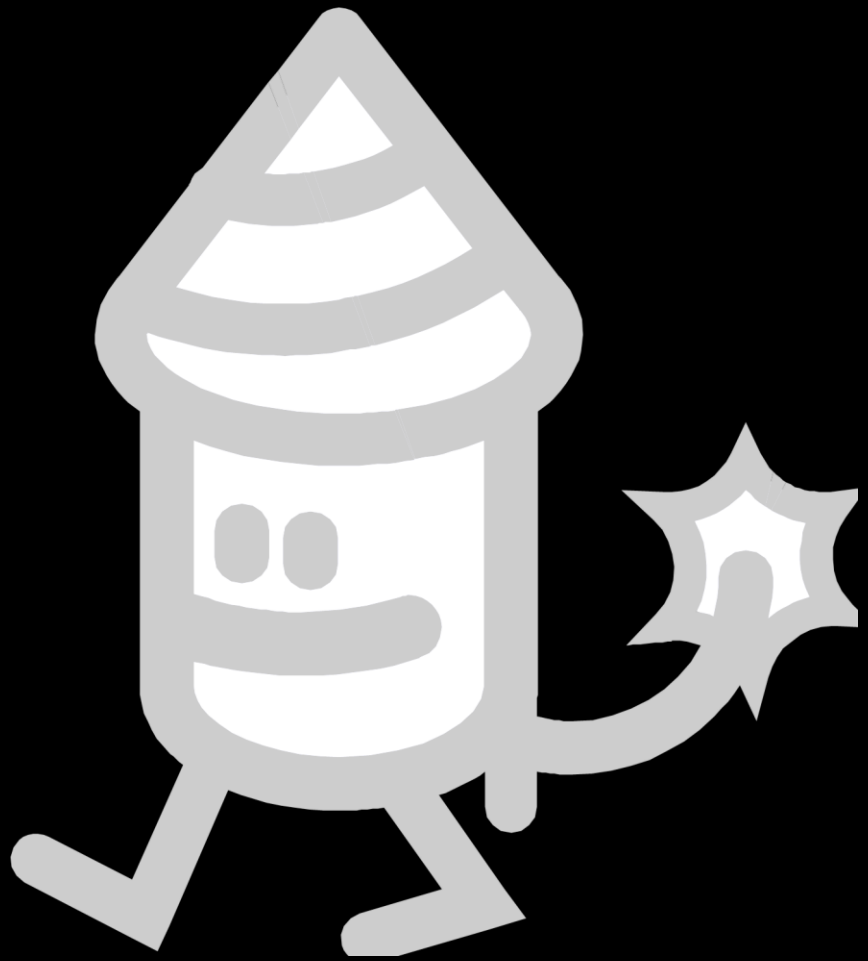
Usual disclaimers

- 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.

Déjà vu all over again



Déjà vu all over again

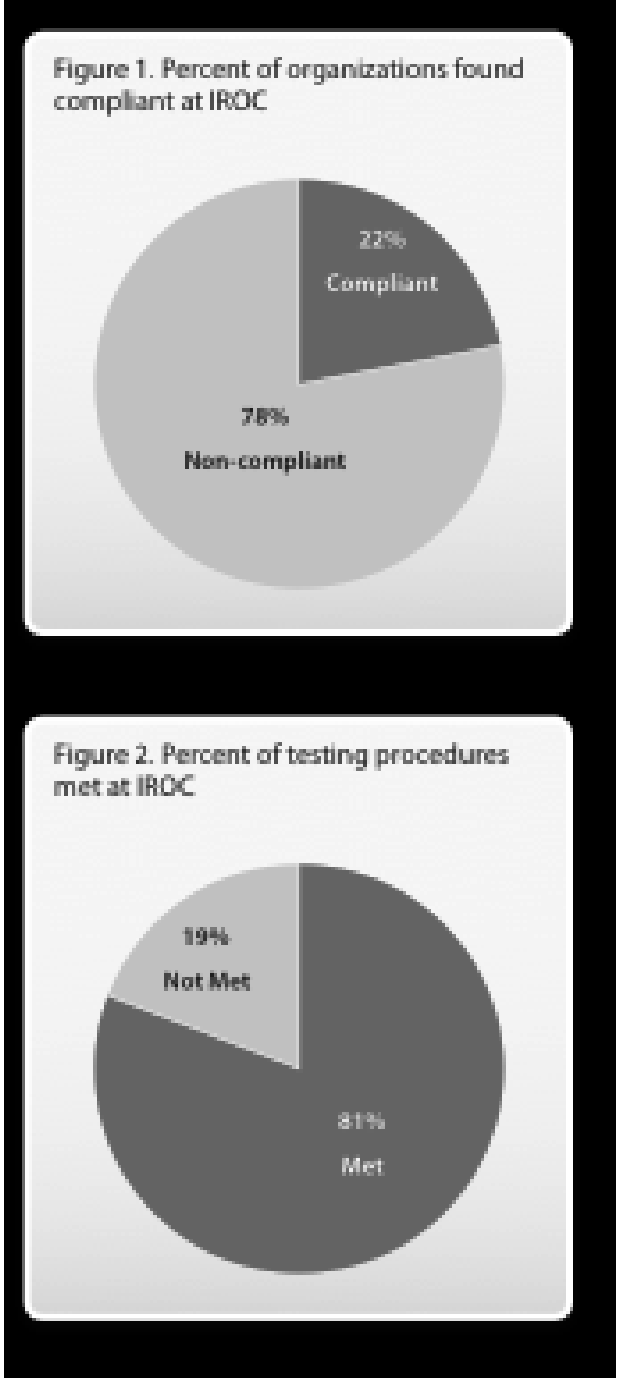


Last year…

- PCI 2.0 was new.
- PCI 2.0 was “fresh”.
- PCI 2.0 was just as frustrating as PCI 1.x.
- PCI 2.0 was still lacking in concrete guidance on a LOT of things:
  - Mobile devices
  - Virtualization
- So…where the hell are we now?

The Good

Becoming Compliant is not easy



So what?

Does Compliance affect “secure” at all?

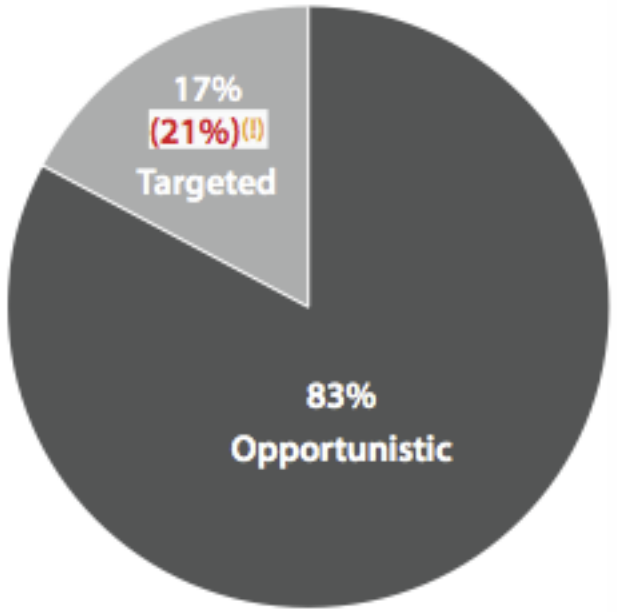
We don’t know how to measure “secure” so the best we can look at is the frequency & characteristics of incidents, and compare those to PCI.

How difficult and targeted were the attacks?

Figure 34. Attack difficulty by percent of breaches and percent of records*

* Verizon caseload only

Figure 35. Attack targeting by percent of breaches and percent of records*



* Verizon caseload only

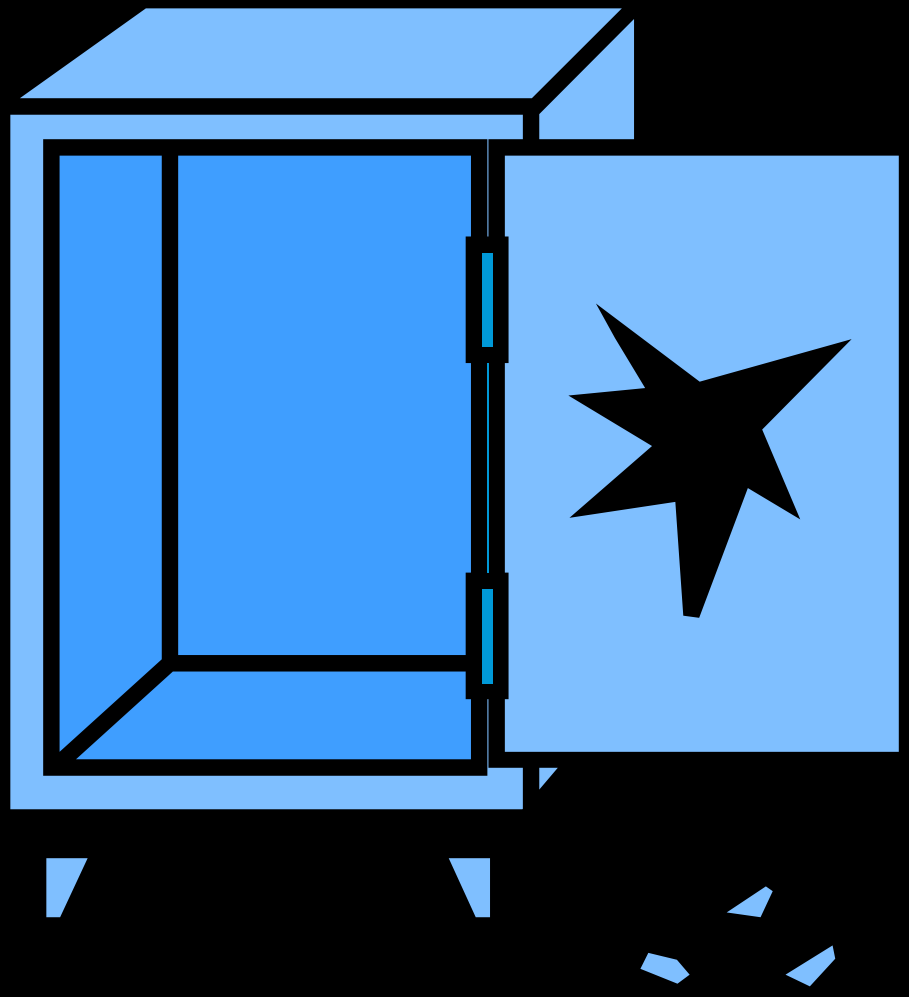
Table 4. Top threat actions based on 2008-2009 payment card breaches investigated by Verizon IR team

Category	Threat Actions	% of Breaches
Malware	Backdoor	25%
Hacking	SQL Injection	24%
Hacking	Exploitation of backdoor or command/control channel	21%
Hacking	Exploitation of default or guessable credentials	21%
Misuse	Abuse of system access/privileges	17%
Hacking	Use of stolen login credentials	14%
Malware	RAM scraper	13%
Hacking	Exploitation of insufficient authorization	13%
Malware	Packet sniffer	13%
Malware	Keylogger / Spyware	13%

Table 16. Percent of relevant organizations in compliance with PCI DSS requirements based on post-breach reviews conducted by Verizon IR team

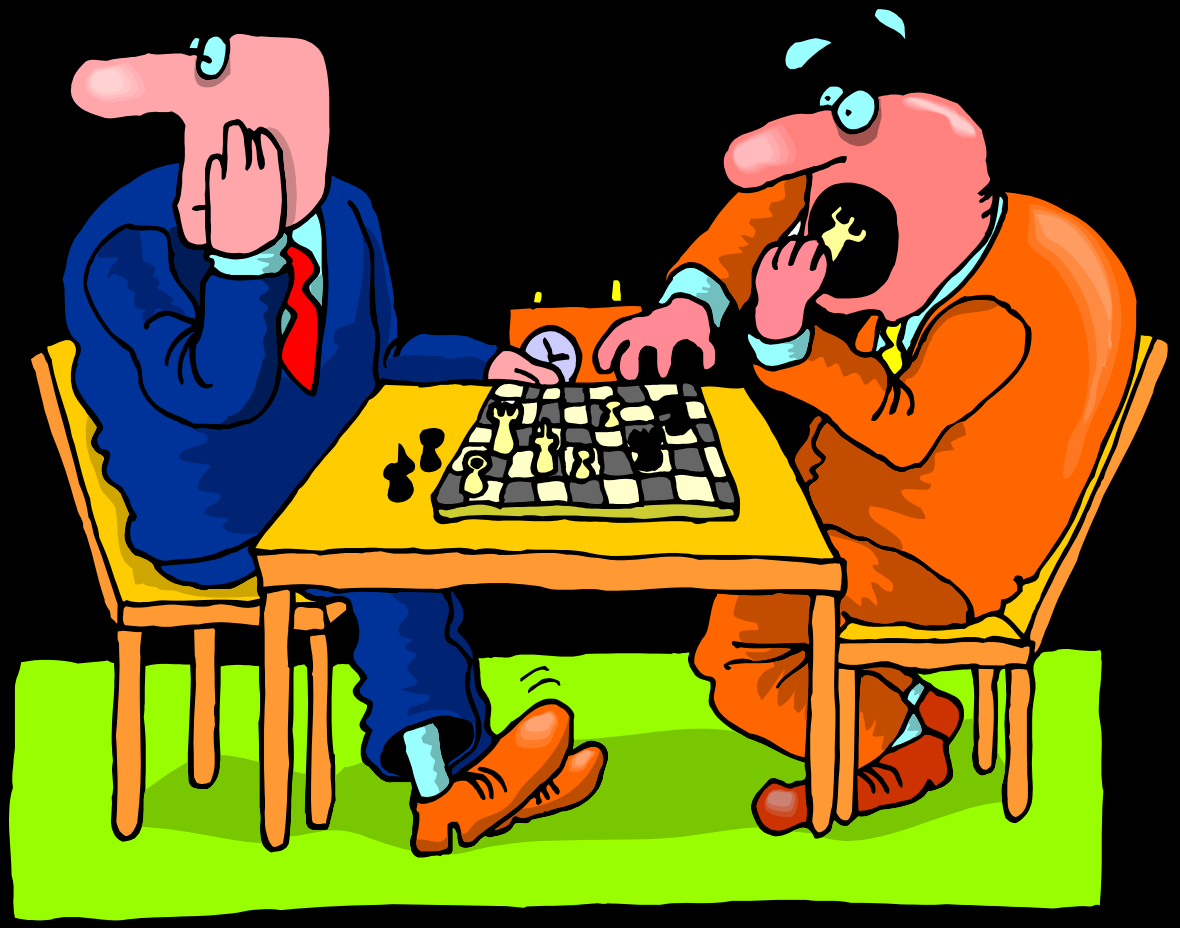
Build and Maintain a Secure Network	2008	2009	2010	PCIR
Requirement 1: Install and maintain a firewall configuration to protect data	30%	35%	18%	46%
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	49%	30%	33%	48%
Protect Cardholder Data				
Requirement 3: Protect Stored Data	11%	30%	21%	43%
Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks	68%	90%	89%	63%
Maintain a Vulnerability Management Program				
Requirement 5: Use and regularly update anti-virus software	62%	53%	47%	70%
Requirement 6: Develop and maintain secure systems and applications	5%	21%	19%	48%
Implement Strong Access Control Measures				
Requirement 7: Restrict access to data by bustiness need-to-know	24%	30%	33%	69%
Requirement 8: Assign a unique ID to each person with computer access	19%	35%	26%	44%
Requirement 9: Restrict physical access to cardholder data	43%	58%	65%	59%
Regularly Monitor and Test Networks				
Requirement 10: Track and monitor all access to network resources and cardholder data	5%	30%	11%	39%
Requirement 11: Regularly test security systems and processes	14%	25%	19%	38%
Maintain an Information Security Policy				
Requirement 12: Maintain a policy that addresses information security	14%	40%	16%	44%

The Bad



The Bad

Sometimes people cheat



The Ugly

Is History Doomed to Repeat Itself?

- We are doing the same %&$# as a decade ago.
- Firewalls.
- SSL.
- Patches (maybe).
- Crypto (sort of).
- Can a WAF save us all!?
  - Ahem.

The Ugly

The Solution(s)?