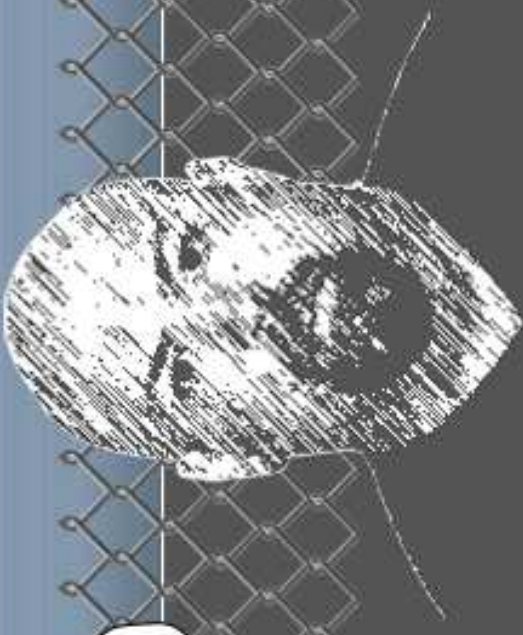


# DWAYNE'S WORLD OF SECURITY



Welcome to Dwayne's World  
Seminar Series

# Agenda



- I. Today's Anti-Rant
- II. Buy the Numbers with Mike
- III. PCI Update
- IV. What SHOULD the PCI process look like
- V. Audit Tips & Common Errors
- VI. Interview – Mike Rothman

[www.businessofsecurity.com](http://www.businessofsecurity.com)

# I. Anti Rant: PCI Ultimatum

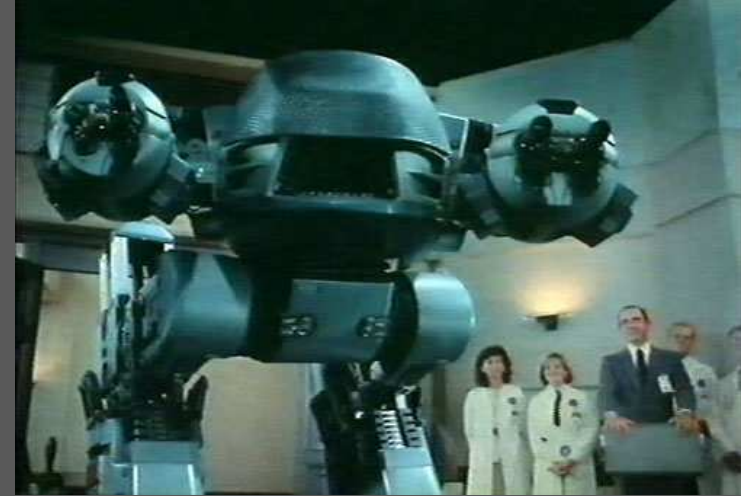


- Ultimatum, your choice

– Comply

– Die

– Lie



## II. Buy The Numbers



(151) Surveyed at PCI Ultimatum Movie Premier

- 63% - Completed Self Assessment
- 54% - Security Policy is Complete and Updated
- 51% - Secured WLAN per DSS
- 49% - Scan for Rogue AP's
- 47% - Encryption Satisfied
- 37% - Credit Card Data Classification (Scope)
- 31% - Engaged a QSA
- 15% - Centralized Logging

## II. Buy The Numbers



- Visa has reported handing out
  - \$4.6M in fines in 2006
  - \$3.4M in fines in 2005
- If breached you also face legal fees, civil lawsuits, and breach related costs that average \$197 per customer record
- And you become a Level 1 Merchant (mandatory audit with QSA involvement)

## III. PCI Update



- **US Level 1 Merchants Deadline WAS Sept 30, 2007 - 77% are compliant (source: VISA January 2008)**
  - 364 Level 1 Merchants (38 were given Sept 30, 2008 extension)
- **US Level 2 Merchant Deadline WAS Dec 31, 2007 – 62% are compliant (source: VISA January 2008)**
  - 1011 Level 2 Merchants (302 were given Dec 30, 2008 extension)
- **Level 3 Merchants – no public deadline – 54% are compliant, 2596 Level 3 Merchants**

## IV. What Should the Process Look Like?



- 1) Check Layer 8 & 9
- 2) Educate Yourself
- 3) Are you a Good General Contractor
- 4) Where is the data
- 5) Define and reduce scope
- 6) Do self assessment
- 7) Engage QSA (or don't)
- 8) Gap Analysis (what's broke)
- 9) Remediate (fix it)

# 1.) Check Layer 8 & 9



- What is the C level attitude / support of PCI Compliance Project
- Is there an executive sponsor, board interest ?
- One version of the PCI project kickoff meeting
  - Letter is straightened out from a crumpled ball and tossed to the IT guy, “Here Johnny, take care of this in your spare time, shouldn’t cost anything eh, sport ?”
- Develop your objectives, strategy and tactics early

## 2.) Educate Yourself



- Congratulations, this Webinar counts (sort of)
- Next, go read some things (all v1.1)
  - Self-Assessment Questionnaire Instructions and Guidelines (which SAQ are you ?)
  - PCI DSS
  - Navigating PCI DSS  
(Understanding the Intent of the Requirements)
  - PCI DSS Security Audit Procedures (DIY)

<https://www.pcisecuritystandards.org/>

## 3.) General Contractor Questions

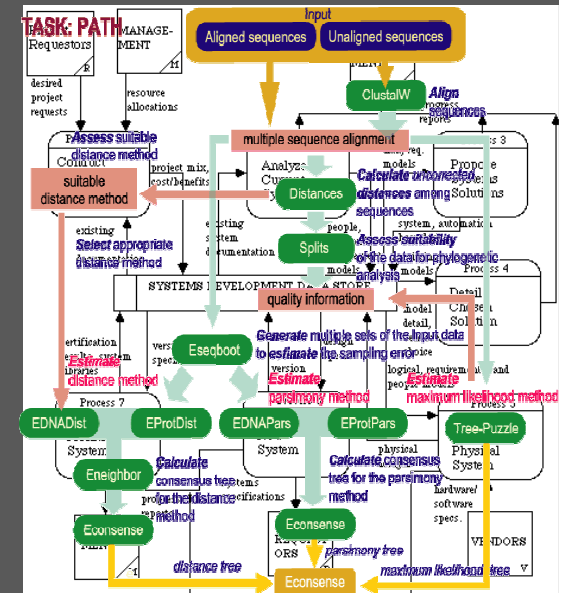


- Do you do remediation? – Run for the hills!
- Tell me about your process ...
  - It better include scope reduction
- Can I get a sanitized ROC ?
- What is your recommendation on self-remediation?
- How do you work with other partners or client IT staff?
- Other contractor type considerations including are you going to self remediate
- You will almost assuredly raise your cost of the QSA if you stumble around blindly trying to comply (or if your implementer does)

# 4.) Where's the Beef ?



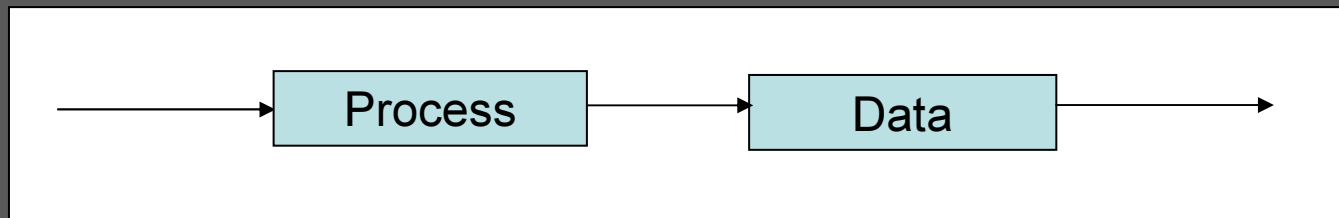
- Where is CC data, where does it flow
- Does data go from structured to unstructured
- Determine necessary applications, services that can be held at one degree of separation
  - DNS
  - Active Directory
  - Management Apps
- Who touches the data ?



## 5.) Define and Reduce Scope



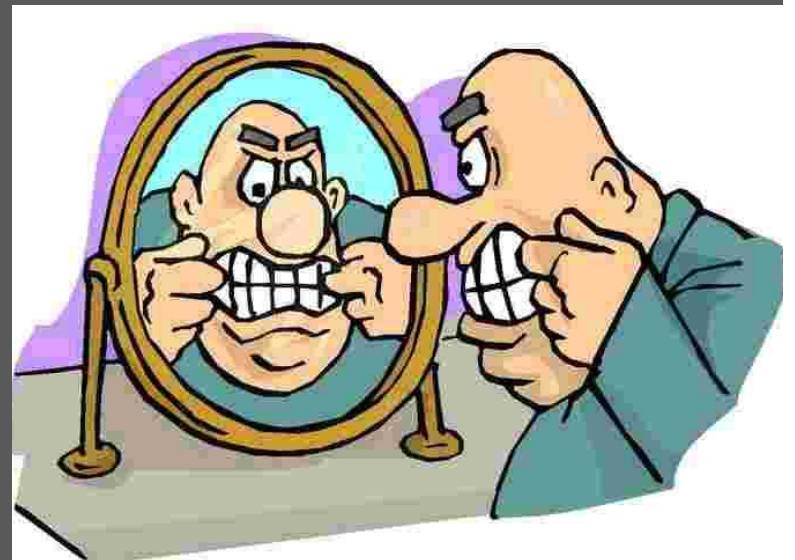
- Based on CC data flows, reduce scope
- VLAN's and ACL's are your friend
- VPN at boundary of CC data scope
- Minimize the number of people and process that have access to the cardholder data
- This helps you save money for PCI DSS
- It also raises your overall security posture



## 6.) Do Self Assessment



- Perform your own Self-Assessment
  - How long will this take
  - Assign a champion
  - You will be able to get funded, and supported
  - **THIS IS IMPORTANT**
- This is instructive and gauges your abilities, if you can't do this, you can't self remediate



## 7.) Engage QSA (or don't)



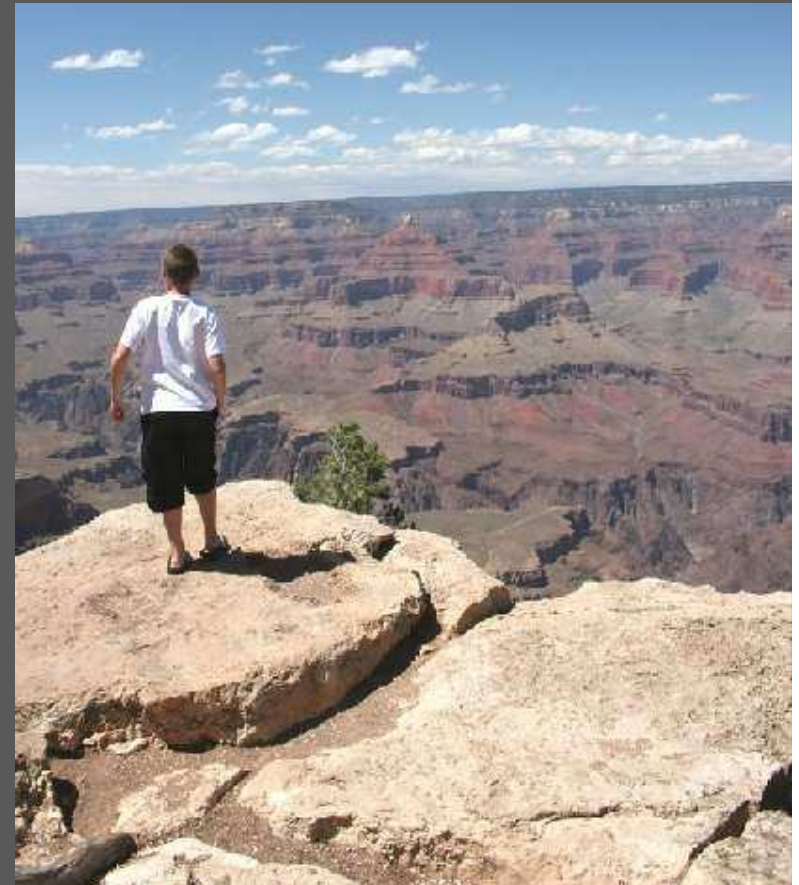
- By now you should have a good handle on your ability to execute with or without a QSA
- Remember the SAP (Security Audit Procedures) contain more than 230 detailed tests
- While budget is important consider the classics
  - DIY always takes more time, education curve
  - DIY takes you away from other tasks
  - DIY means you might make mistakes
  - DIY means you might learn more, be better at your job and have a greater sense of accomplishment

# 8.) Gap Analysis



- Figure out what's wrong, document it
- Use correct PCI SAQ 11, 21, 38 or 228 Questions

Type	Description	SAQ
1	Card-not-present merchants, all functions outsourced	A
2	Imprint-only no data storage	B
3	Stand-alone dial-up terminals no storage	B
4	POS to Internet, no storage	C
5	All other merchants and all service providers	D



Source – PCI DSS Instructions and Guidelines

## 9.) Remediate



- Fix it, if you are a DIY, use the Audit Guide to help you
- SANS also teaches a good 2 day course

Audit 521 - Meeting the Minimum: Standard for Protecting Credit Card and Other Private Information PCI CISP: The Visa Digital Dozen

# V. Auditing Tips



- This is NOT an adversarial relationship
- Auditors/Assessors like clear well organized:
  - Policies and procedures
  - Up to date documentation
  - Reports
  - Chain o' command
  - Real adherence to policy
  - Accountability
- They don't like – The opposite

# V. PCI Assessment Failures



PCI Requirement	Percentage Failing
#3 Protect Stored Data	79
#11 Regularly test security systems and processes	74
#8 Assign a unique ID to each person	71
#10 Track and monitor all access to network resources and cardholder data	71
#1 Install and maintain a firewall configuration to protect data	66

Source: VeriSign sample of 112 assessments, 30 ultimately passed and 82 did not

## V. Common Data Breach Failures



- Approximately 50% of data breach failures are theft of laptops (majority) or media
- [www.attrition.org](http://www.attrition.org) good source of information
- PCI as framework for other data security projects



Interview Time ...

Mr. Mike Rothman  
President and Principal Analyst  
Security Incite

<http://securityincite.com/>

Check out the Intro  
and get  
**5 TIPS TO BE A  
BETTER CSO**  
**FOR FREE!**

The Pragmatic  
**CSO**  
INTRODUCTION

12 Steps to  
Being a  
Security Master

By Mike Rothman

The image shows a book cover for 'The Pragmatic CSO Introduction' by Mike Rothman. The cover features a cartoon character in a suit standing on a path that leads to a city skyline. The text on the cover includes 'The Pragmatic CSO Introduction', '12 Steps to Being a Security Master', and 'By Mike Rothman'. There are also several small icons representing different security concepts.