Meet the Owner of a Real Hacked Company - Forensic Analysis

Mark Shelhart
Forensic Practice Manager
Agenda

- Trustwave
- Company Background
- PCI terminology
- Notification
- Incident Response
- The Attack
- Remediation and Reaction
Trustwave

- Company information
Company Profile

- Jimmy’s business
- Jimmy’s clientele
Credit Card Compromise Definitions

- PCI-DSS
- Common Point of purchase
- Track Data
The Phone Call

- Bank’s notification to the company
- Initial reaction the call
- What PCI means at this point
- Involvement from law enforcement
- Local customers media coverage
Incident Response

- How hard it was to lock things down

- Deficiencies found
  - Reality vs perceived security

- The launch of the investigation

- Working with the investigation team
  - What was needed
  - What was learned in flight.
The Attack

- Initial attack vector
- Tools used
- Obfuscation – none
- Harvesting of data
EnCase Screenshot #1

• Pending review
EnCase screenshot #2

• Pending review
Remediation & Reaction

• What was left to lock down

• Cost
  – The investigation and lockdown
  – Fines by the card associations
  – Customer Fraud

• Lessons learned
Questions?