

Information Security Roundtable Forum

Countermeasures to Identity Theft: Protecting Critical Customer & Employee Data

Moderators/Introductions

- Welcome
- Robert Nolan-Sales/Marketing Manager, Pivot Point Security
- Introduction: John Verry-Principal Enterprise Security Consultant, Pivot Point Security

About these Presentations

- Will not be “Death by Power Point”
- Dialogue (not Monologue)
- Goal is to introduce key concepts and get the session to be interactive
- Educational seminar – not a Sales & Marketing exercise

Shaping the Presentation

- Understand the audience
 - Roles
 - Reason/goal for being at session

A Sad State of Affairs

- Bank of America - 1,200,000 records
(Federal Employees, even US Senators!)
- Lexis Nexis - 310,000 records
- Ralph Lauren - 180,000 records
- Choice Point - 150,000 records
- DSW Shoe Warehouse - 145,000 records
(750 confirmed fraud cases)
- Las Vegas DMV - 9,000 records

What Happened?

- **Bank of America** - “Lost” data tapes; possibly stolen by commercial air baggage handlers
- **Lexis Nexis** - Social Engineering (fraud), unspecified breakdown of internal customer credentialing process
- **Ralph Lauren** - Not specified yet, but associated with a “US-based retailer”, according to MasterCard
- **Choice Point** - Social Engineer & Fraud; via forged documents such as business licenses, thieves became a Choice Point “customer” and gained access to customer data
- **DSW Shoe Warehouse** - “Traditional” technology hack; details not disclosed
- **Las Vegas DMV** -Physical break in/theft of computer containing 3 months worth of drivers license data (SS #, photo, signatures, names, age, etc.)

Personal Identity Theft Experience

- Three Different Examples of Identity theft
 - Hack of Confidential Patient Health Information from Health Care Provider
 - Hack of Credit Card Data from NPO
 - Hack of Client Data from International Bank
- Three Distinctly Different “causes”
- Three Distinctly Different Solutions
- There is no Silver Bullet

Identity Theft via Network Hack

- Large Health Care provider looking for HIPAA validation
- Application & systems hosting application were highly secure
- Cisco switches had older IOS software
- VoIP Telephones running older software
- “ARP Spoofed” the switch to see a copy of all network traffic including clear text passwords
- Recorded privileged conversations between clients, doctors and Health Care Provider
- Gained access to full client health data
- Solution: Network Configuration Management, Risk Assessment modifications

Emerging Technical Controls for Identity Theft

Alter Point

- Network Configuration Management
 - Enforces Policy and Procedure for Network Devices

Alterpoint

Network Security Through Network Change & Configuration Management

- **David Johnson, Director Customer Services**

Identity Theft via Database Hack

- International Bank had concerns re hosted Fund Transaction system
- SQL Server back end running vulnerable services
- Used ISQL vulnerability to create Admin User on System
- Elevated access to DB Admin
- Garnered access to hundreds of high value clients (\$500M)
- Solution: Database Monitoring Policy, Data Classification and Data Ownership Policy updates, Database Intrusion Protection Software

Emerging Technical Controls for Identity Theft

Application Security Inc.

- Database Intrusion Protection
 - Provides ongoing monitoring of Database for vulnerabilities and access falling outside policy
 - Identifies Vulnerabilities
 - Actively Prevents Attacks

Application Security, Inc.

Protecting Customer Data

- Aaron C. Newman, Founder & CTO

Identity Theft via Application Hack

- NPO had rolled out new donor web portal
- System and Network were highly secure
- App was subject to SQL Injection (Select *) & Forceful browsing to Administrative Interface
- Retrieved 1,000 + user names, donation history, and credit card data
- Solution: Security Testing Policy, Data Classification Policy, Application Firewall

Emerging Technical Controls for Identity Theft

F5 Networks-TrafficShield

- Application Firewalls
 - Front ends Web Applications and blocks malicious attacks
 - Can be use for problematic application (vendor provided, under development, short term protection)
 - Can be used long term on critical applications

F5 Networks

Securing Your Applications

- Marc Kaplan, Sr. Security Engineer

Good News – Identity Theft is Usually the Breakdown of Multiple Controls

- Identity Theft is usually the result of a breakdown of multiple levels of the control environment
 - Administrative Controls (Executive Management – think policies & strategic planning)
 - Operational Controls (Business/IT Management - think procedures & tactical planning)
 - Technical Controls (IT Personnel – think devices/systems and their administration)
- Holistic View Necessary
- Your client data lives inside your Information Systems Control Environment
- How do you take accountability for Data Security ?
 - Information Technology Governance

Wrap Up

- Q & A
 - For more info on any of the presentations/solutions today please contact
 - jverry@pvtpt.com / (732) 267-6324
 - rnolan@pvtpt.com/ (609) 890-1131 xt. 321
 - Thank you.

Giveaways

- 1st Place: Creative Zen Micro 5GB MP3 Player (+ *partner giveaways*)
- 2nd Place: Pivot Point Security PING Golf Shirt (+ *partner giveaways*)
- 3rd Place: (2) Pivot Point Security Hardcover Journal books w/ pen, calendar & contacts page (+ *partner giveaways*)