AFP®
Annual Conference

Association for Financial Professionals®

November 7-10, 2010 | San Antonio

ORIGINAL
ESSENTIAL
UNBIASED
INFORMATION

# Information Security – It's more than just PCI

Terry W. Crawford
Senior Vice President & Treasurer
AMC Entertainment Inc

Rue Jenkins
Assistant Treasurer
Costco Wholesale Corp

# Agenda

- Roundtable discussion format
- Set the stage
- Questions to ponder – What questions do you have?

# AMC Entertainment Inc. Overview

- One of the world's largest and most innovative theatrical exhibition companies
  - ➢381 theatres, 5,325 screens
  - ➢$2.7B revenues, $388M Adj. EBITDA
  - ➢227M attendance
  - ➢invented megaplex, most modern cinema amenities
  - ➢Leader in deployment of premium formats
- Operates in an attractive industry with stable long term fundamentals and strong near-term growth, driven by premium formats, digital expansion and improved food & beverage options
- Predominately a major market operator with industry leading theatre-level metrics
- Ideally positioned to capitalize on growth opportunities, with a unique balance of tenured and industry diverse executives, highly productive assets and proprietary initiatives

# Costco Wholesale Overview

- 3rd Largest retailer in U.S.
- 8th Largest retailer in the world
- Over $70B in sales
- 569 Warehouses worldwide
  - 415 US  154 International
- 1.7M transactions / day
  - 56% Plastic  41% Cash / Check

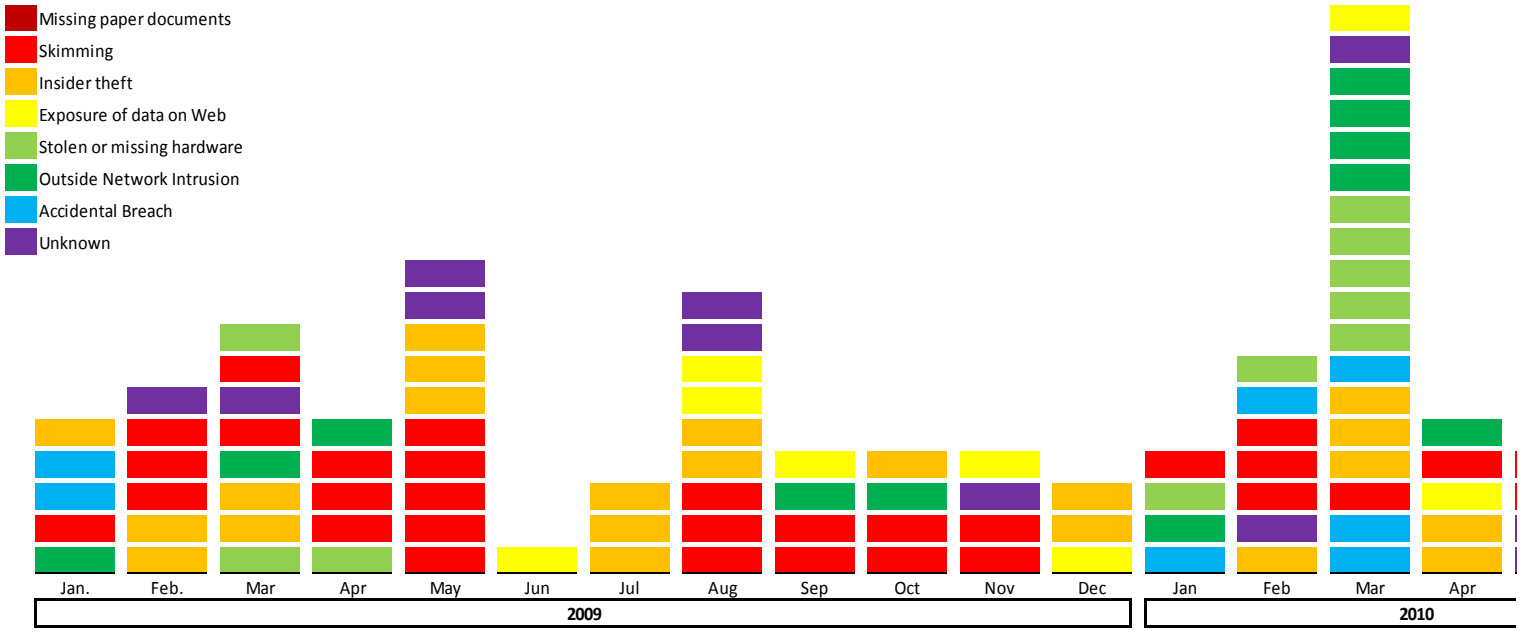
# Payment Types

| | Credit Card | Pin Debit | Sig Debit |
|---|---|---|---|
| Whse | AX, HSBC | All | V, MC |
| FSA/EBT | | EBT | FSA |
| Gas | AX, HSBC | All | |
| Online | AX, V, MC, D<br>HSBC | N/A | V, MC |
| Travel | AX, V, MC, D<br>HSBC | N/A | V, MC |

# Personally Identifiable Information -- PII

- Card Associations / Issuers:
  - VISA, MasterCard, American Express, Discover
  - HSBC (private label credit card)
- Networks:
  - Interlink (VISA), Maestro (MasterCard)
  - Pulse (Discover), NYCE, Star, CU24, Excel,
  - AFFN, Alaska Option, Jeanie, Shazam, ATH
- Membership/Loyalty
- Employee Data
- HIPAA
- Vendor Information

# 2009/2010 Data Breaches Timeline




*Source: www.bankinfosecurity.com*

# Did you know?

| | |
|---|---|
| 285 | Million records were stolen in 2008[1] |
| $225 | is the average cost per record breached due to malicious acts[2] |
| 67% | of data breaches happen because of mistakes by well-meaning insiders[3] |
| | 1. Verizon Business Risk Team, ***2009 Data Breach Investigations Report***<br>2. Ponemon Institute, ***Cost of a Data Breach Study, 2008***<br>3. Verizon Business Risk Team, ***2009 Data Breach Investigations Report*** |

# Cost of a Data Breach

- Total cost of a data breach continues to increase every year, increasing from an average of $197 per record in 2007 to $202 per record in 2008
- Abnormal churn or customer turnover is key factor driving increased cost. Over the last 4 years lost business component grew by more the $64 on a per victim basis
- Average organizational cost of a data breach in 2008 totaled $6.65 million, up over 4% in just one year
- 43 data breaches reported in 2008 with the largest costing more than $32 million
- Data breaches concerning lost laptops are more expensive than all other incidents, costing $249 per victim versus $177 per victim for all others

*Source: Ponemon Institute Fourth Annual US Cost of Data Breach Study*

# Think digital – Where to look

- Any digital device can carry or store confidential information
  - Laptops --  Highest cost per victim
  - PDA's
  - Jump drives
  - Copiers – Consider retail or remote locations

# AMC Case Study – Marketing Agreement

- Marketing Department entered into an agreement with a third party marketing firm
  - ✓ Provides a new and exclusive marketing channel
  - ✓ Only investing in measurably incremental sales
  - ✓ Placing category exclusive messages in communications to marketing company's affinity partners, generating 320+ million impressions per year
    - ➢ Email marketing campaigns
    - ➢ Statement inserts
    - ➢ In-branch merchandising
    - ➢ Various other materials with card partner marketing channels
  - ✓ Merchant funded program with more than 40mm consumers incented to use cards issued by card partners to earn rewards faster

# AMC Case Study – Marketing Agreement

**Member visits AMC and uses their program card**

- Data transmitted for auth. and settlement
- Card data to marketing company to match members

**Marketing company warehouses and stores data for 6 months**

- Data storage actually outsourced to another provider
- Off site file storage company also receives and stores data

**Marketing company matches purchase transactions with issuer data**

- Marketing company sends shopping rewards to program members point bank for redemption
- Member receives email confirmation of their reward for visiting AMC

# Costco Case Study - What data?

- Identify the data?
- Where is the data being stored?
- Where is the data being sent?

# Date Loss Prevention: A Solution to Prevent Data Breaches

| | | | | |
|---|---|---|---|---|
| Well Meaning Insiders<br><br>**84% of Breaches!** | Sensitive Data exposed on systems, servers, desktops | Lost or stolen laptops | Email, Web Mail, Removable Devices | Out of date Business Process |
| Targeted Attacks | Incursion (SQL Injection) | Discovery (sniffer) | Capture (duplicate) | Exfiltration (sending captured data) |
| The Malicious Insider | White Collar Crime | Terminated Employees | Career Building | Industrial Espionage |

# Prevention Steps[1]

- Protect information proactively
- Automate review of entitlements
- Identify threats in real time
- Stop targeted attacks
- Prevent data exfiltration
- Integrate security operations

1 symantec – Causes of Data Breaches

# Data Loss Prevention -- Implementation

- **Assemble a Data Security Team and Assess the Data**
  - Cross functional team, IT, finance, legal, procurement, risk, operations, etc
  - Determine the scope of data maintained
  - Identify how data is collected, used and transmitted
  - Indentify data security threats
- **Develop Data Protection and Privacy Policies and Procedures**
  - Review existing policies and conform with best practices
  - Address social networking sites, LinkedIn, Twitter, Facebook, employees "chatting" are inadvertently handing "hackers" the inside information needed to penetrate corporate networks.
    - Block or institute strict policies to avoid becoming next victim
- **Monitor Sensitive Data, Not People**
  - Credit Cards (face-to-face / online)
  - Social Security Numbers (P/R)
  - Bank Accounts (Treasury, A/P, P/R)
  - Customer / Member personal information
  - Other Future: HIPAA, other business data

# Data Loss Prevention -- Implementation

- **Track Key Data Through the System**
  - Email, FTP, USB drives, CD's
  - Where is the data stored
- **Train, Test, Update and Monitor Policies**
  - Test at least quarterly
  - Formally train all employees on the risks

# How to respond – Mitigate Risk

- Contractually allocate liability
  - Contracts with vendors should specify they are liable for breaches of data in their control
- Develop a response plan
  - Cross functional team, IT, finance, legal, procurement, risk, operations, etc
  - Forensic experts – identify who you would use in case of a breach
  - Legal experts – identify who you would use to navigate jurisdictional requirements
- Consider insurance
  - What is your corporate risk appetite – low frequency/high severity situation
  - Make sure coverage is what you really think it is

# Resources

- American National Standards Institute – The Financial Management of Cyber Risk
- Information Law Group – www.infolawgroup.com
- Data breach articles – www.bankinfosecurity.com
- PCI standards
- CSO – www.csoonline.com