Cybersecurity In The Retail Sector

- Erik Buschardt

- **Background:** Undergrad in Computer Science, 15+ years in retail and hospitality industries.

- **Goal:** Masters at Webster in #CyberSecurity to enhance, learn about and secure retail services available to public and private sectors, across wide variety of industry, military, private hospital networks, public education, finance, etc.

Cybersecurity In The Retail Sector

- **Scope and Magnitude – By The Numbers**

- While #CyberSecurity has global implications in a wide variety of industry as per media news outlets and breaking news, we will focus our discussions on the American private economy and retail consumer base.

Cybersecurity In The Retail Sector

- **Scope and Magnitude (Continued)**
- Target Corp (Nov-Dec 2013)
    - 70 M demographics stolen (ID)
    - 40 M CC stolen
    - Auto-issuance of new CC and DC cards.
    - Offered credit monitoring for one year,
      https://corporate.target.com/article/2014/01/free-credit-monitoring-and-identity-theft-protecti

Cybersecurity In The Retail Sector

- **Scope and Magnitude (Continued)**

- Neiman Marcus (July-Oct 2013)

  – 350,000 CC stolen, 9K used fradulently

- Michael's / Aaron Brothers (May 2013-Jan '14)

  – 2.6 M CC affected, (400K in AB)

  – Vulnerability included POS terminals as entry point for exploit.

Cybersecurity In The Retail Sector

- **Scope and Magnitude (Continued)**

- Ebay (Feb-Mar 2014) – 233 M cust affected.

  - Vulnerability included old passwords for employee login credentials.

  - Public statement asking all users to change pw, (https://www.ebayinc.com/stories/news/ebay-inc-ask-ebay-users-change-passwords?)

Cybersecurity In The Retail Sector

- **Scope and Magnitude (Continued)**

- PF Changs China Bistro (Sept 2013-June '14)

  - 33 resturants affected, ID info sold.

- UPS (Jan-Aug 2014)

  - 60+ UPS Stores affected including CC #s

  - Result of **Backoff POS malware...**

  - *https://www.us-cert.gov/ncas/alerts/TA14-212A*

Cybersecurity In The Retail Sector

- **Scope and Magnitude (Continued)**
- Home Depot (Sept 2014)
  - 56 M cust CC affected, 2K stores in NA.
- Goodwill Ind Intl (Feb 2013-Aug 2014)
  - 868,000 CC/DC#s stolen from 330 stores
  - Malware suspected through 3rd party vendors

Cybersecurity In The Retail Sector

- **Scope and Magnitude (Continued)**
- SuperValu *(Cub Foods, Shop&Save, FarmFresh)*
    - 1st attack June/July 2014
    - Malware affected cust data and CC data
    - 2nd attack late Aug/Sept 2014
    - Only payment card data affected.

Cybersecurity In The Retail Sector

- **Scope and Magnitude (Continued)**
- JP Morgan Chase (financial retail)
  - Attack in June 2014, not noticed till Aug.
  - 76 M households, 7M smallbiz affected
  - Hackers likely orig from Russia
  - Suspected ties to Russian govt

Cybersecurity In The Retail Sector

- **Scope and Magnitude (Continued)**
- Dairy Queen Intl / Orange Julius smoothies
  - 395 restaurants affected, CC/DC stolen
  - Backoff malware suspected... (again!)

Cybersecurity In The Retail Sector

- **Cultural Norms in 21st Century – ID Theft**

- As we see more retail outlets hacked and more consumer data compromised, a new de facto norm is created re: Personally Identifible Info

- Some cultural references: Hollywood movies

  - The Net (1995); The Jackal (1997), Ocean's 11 (2001) et al.; Mission Impossible franchise (1996, 2000, 2006, 2011, 2015); Catch Me If You Can (2002), Idendity Thief (2013).

Cybersecurity In The Retail Sector

- **Cultural Norm – Precautions & Resolutions**

- Websites using cookies; user acceptance rate

- Email promotions and spam

- FBI and other agencies involved

  - Creation of academic programs such as ours – *Dr. Johnson's background with USSS NY and SanFran field offices, FBI, Electronic Crime Task Force...* - (*http://www.webster.edu/business-and-technology/about/leadership/*)

Cybersecurity In The Retail Sector

- **Cultural Norm – Precautions & Resolutions**
- What can you do as a consumer?
  - Check credit rating **free once per year**
    - AnnualCreditRating.com (per FTC)
  - Monitor accounts periodically for abuse.
  - Don't ignore consumer warnings on media regarding ID breach attacks.

Cybersecurity In The Retail Sector

- **Cultural Norm – Precautions & Resolutions**

- What can the government do?

  - FBI Cyber Division (since 2002)

    - Heads national effort to investigate and prosecute internet crimes including "...terrorism, espionage, intrusions and major fraud"

  - Immigrations & Customs Enforcement (DHS)

    - Cyber Crimes Center (C3) – *Formed 1998*

Cybersecurity In The Retail Sector

- **Cultural Norm – Precautions & Resolutions**

- Summary, <u>Thank You and Questions</u>:

  - Retail and online shopping precautions

  - DC/CC safety, banks and agencies offer protection (such as Lifelock, ProtectMyID/Experian in the case of Target)

  - CC: fraud protection - "did not buy that", vs. DC safety

  - Annual credit check and basic personal finance safety – monitor your purchases (usu. 30-60 days, varies by bank).