The Millennium Alliance – Executive Roundtable

January 28th at Noon

" Takeaways from the Top Cybersecurity Breaches of 2024: How Can We Better Prepare in 2025"

Moderated by:

Dave Chatterjee, Ph.D.

Author: Cybersecurity Readiness: The Holistic and High-Performance Approach

Host, The Cybersecurity Readiness Podcast

https://www.dchatte.com

https://www.linkedin.com/in/dchatte/

Agenda and Discussion Plan

1. **Introduction (5-10 min)**

2. **Significant Breaches in 2024 (15 min)**

    - The following have been reported to be the most significant breaches in 2024?
        i. National Public Data breach: 2.9 billion records
        ii. AT&T breaches: 50 billion+ records
        iii. Ticketmaster breach: 560 million records
        iv. Change Healthcare breach: 145 million records
        v. Dell breach: 49 million records

    Which of these (or any other) got your attention and why?

3. **Organizational Weaknesses and Vulnerabilities Exploited (15 min)**

    - What were some organizational weaknesses and vulnerabilities exploited?

4. **Lessons and Key Takeaways (15 min)**

    - What are some lessons and key takeaways from these breaches?

5. **Concluding Thoughts (5-10 min)**

Recommendations and Best Practices

Sources

1. Cybersecurity Readiness Podcast (www.cybersecurityreadinesspodcast.com) -- Excerpts from Dr. Dave Chatterjee's conversations with CEOs, CISOs, and other subject matter experts.
2. Research and practitioner articles.

I. Significant 2024 Breaches

National Public Data Breach: 2.9 billion records

- National Public Data, an online background check and fraud prevention service, experienced a significant data breach in April 2024.
- Cybercriminals discovered a zip file on the NPD website with plain-text usernames and passwords needed to access the database. Sensitive data, including names, social security numbers, phone numbers, and physical and email addresses, was leaked on the dark web.
- The incident affected approximately 170 million US and Canadian citizens, and NPD's owner is now facing more than a dozen lawsuits related to the breach.

AT&T Data Breach: 50 billion plus records

- AT&T experienced multiple data breaches in 2024 that exposed customer contact details and account-related information due to vulnerabilities in third-party vendor systems.
- Criminals stole the records of "nearly all" of AT&T's cellular and landline customers—approximately 50 billion customer call and text records in total.

Ticketmaster Breach: 560 million records

- Between April and May 2024, attackers managed to exfiltrate 1.3 terabytes of data from Ticketmaster after they gained access to a cloud database hosted by third-party data services provider Snowflake. Leaked data included customer names, email addresses, payment information, and purchase histories.
- The breach went undetected for nearly seven weeks, delaying Ticketmaster's regulatory notification until June 28. Customers were not made aware of the breach until mid-July — almost two months after it had been discovered.

- The incident and Ticketmaster's delayed response has led to significant fallout, affecting over 40 million users and leading to multiple lawsuits, including class action suits and filings from the U.S. Justice Department against Ticketmaster's parent company, Live Nation.

Change Healthcare breach: 145 million records

- In February 2024, Change Healthcare suffered the largest known data breach of protected health information to date, affecting more than 100 million Americans. The breach exposed Social Security numbers, driver's license numbers, medical records, insurance data, and financial and banking records — and caused widespread disruptions in processing payments and prescriptions across the US healthcare system.

- The parent company of Change Healthcare has faced significant financial repercussions, with direct response costs totaling $1.5 billion and overall cyberattack impacts reaching $2.4 billion, including a $22 million ransomware payment made in exchange for a promise to destroy the stolen healthcare data.

- The breach was caused when attackers either stole or purchased credentials for a Citrix portal used for remote access to Change Healthcare systems, which did not have multi-factor authentication in place.

5. Dell breach: 49 million records

- Dell Technologies experienced a significant data breach this year in which attackers gained access to customer information, including names, email addresses, and hashed passwords.

- This breach originated from a brute-force attack launched after a hacker accessed a client portal via one of Dell's resellers. The attacker then sent over 5,000 login requests per minute for nearly three weeks, totaling almost 50 million attempts, yet Dell's systems failed to detect this activity. It was only after the hacker sent multiple emails to Dell about the security vulnerability that the company became aware of the breach**.**

II. Lessons/Key Takeaways

1. Hands-on Top Management

2. Creating a We-Are-In-It-Together Culture

    - Building emotional capital (among employees and business partners)
        - Feeling valued
        - Developing a sense of belonging
        - Taking pride in their work
        - Having fun
        - Perceiving leadership to be genuine and authentic

    - Incentivizing behavior

3. CISO Empowerment

    - There is growing recognition that the CISO is much more than a risk or technology officer. They are business enablers and must be involved in strategic and value creation activities.

4. Joint Ownership and Accountability

    - Business partners, third-party service providers, and vendors must share responsibility for protecting sensitive data

5. Comprehensive Asset Discovery

    - The Cybersecurity and Infrastructure Security Agency recently issued a directive (BOD 23-01) requiring federal enterprises (civilian executive branch) to perform automated asset discovery every 7 days

    - There are many hurdles associated with asset inventory management. The one that looms the largest is unmanaged devices, unmanaged assets, the Achilles heel of any asset inventory program.

6. Defense-in-Depth Approach

    - Physical, Technical, and Admin controls

7. Awareness and Training

    - Role-based
    - Incremental and Continuous
    - Engaging and Interactive
    - Important component of performance review

8. Continuous Monitoring and Prompt Action

    - Thorough logging of monitoring results, actions taken, and decision-making rationale

9. Highly Rehearsed Response and Recovery Capability

10. Real-time Security Audits and Drills