TOP BREACHES of 2014

Dec. 2013 to Dec. 2014

If the top breaches of 2014 taught the security world anything, it's that size and sector don't matter. All organizations are vulnerable to external attack, and the consequences can derail organizations and their leaders' careers. Here's a look at the top incidents of the year and the lessons security experts gleaned from them.

6

CHS Community Health Systems

4.5 MILLION PEOPLE AFFECTED

Information compromised: Names, addresses, birthdates, telephone numbers, Social Security numbers

Description: The largest health data breach in 2014 saw a suspected hacker group from China breaching the organization's systems and pilfering sensitive patient details. The attack offered more proof that hackers are focusing on healthcare organizations, as they're perceived to be easier targets than other sectors.

5

THE HOME DEPOT

56 MILLION PEOPLE AFFECTED

53 Million email addresses also stolen

Information compromised: Credit and debit card numbers

Description: Home Depot's breach resulted from the compromise of a third-party vendor, a fact that is "eerily" similar to the circumstances of the Target breach. This points to the need for organizations to more closely monitor the security measures of their vendors and ramp up breach detection efforts, experts say.

4

JPMorganChase

76 MILLION PEOPLE AFFECTED

Information compromised: Names, addresses, phone numbers, e-mail addresses

Description: A massive breach against Chase likely started with a server the bank's security team overlooked when upgrading to two-factor authentication controls. The takeaway from this incident is that if the nation's largest bank (which was considered to be among the most secure organizations in the world) can be breached, then virtually all other banking institutions must be considered at risk.

3

TARGET

110 MILLION PEOPLE AFFECTED

Information compromised: Credit and debit cards, customer details

Description: Although the breach occurred in 2013, Target's incident was a major talking point throughout 2014, as the company faced massive breach response costs, a changing C-suite, federal scrutiny and several class action lawsuits. Target's breach showed that such incidents can cost a CEO's job, and it proved to be the watershed event that kicked off a year that saw several large-scale card breaches.

2

ebay

145 MILLION PEOPLE AFFECTED

Information compromised: Encrypted passwords, customer names, e-mail addresses, mailing addresses, phone numbers, dates of birth

Description: This breach, which originated after a small number of employee log-in credentials were compromised, impacted a massive number of customers, and sparked investigations from state attorneys general and the UK Information Commissioner's Office. Yet, surprisingly, it remains perhaps the least-discussed major breach of 2014.

1

UNKNOWN PEOPLE AFFECTED

Information compromised: PII, PHI, unreleased feature films, company e-mails

Description: As the dust continues to settle more than a month after the film studio was hit with a massive "wiper" malware attack that exposed intellectual property along with personal employee details - and led to a heated debate over whether the hack was launched by North Korea – the breach could serve as a major turning point, giving CISOs a new degree of board-level visibility for their security strategies and investments.

SONY PICTURES™

To learn more about data breach response, prevention and detection, visit www.databreachtoday.com.

Data Breach TODAY

Prevention. Response. Notification.