Top 10 Data Breaches of 2010

January 21, 2011
By Lisa Phifer

Submit Feedback »
More by Author »

No organization wants to make breach headlines; many have spent considerable sums to avoid them. And yet, huge data breaches are still being reported. The Identity Theft Resource Center catalogued 662 breaches in 2010, exposing more than 16 million records.

Back in 2009, Heartland took first place by losing 130 million records to one SQL injection attack. At first glance, last year's tally looks much better. But many breaches are disclosed without record counts, and those counts tell only part of the story. So how did we really fare last year?

10. Affinity Health Plan: 29 percent of breaches tracked by ITRC were disclosed due to reporting laws. For example, Affinity Health's breach involving 409,000 records was reported to comply with Department of Health and Human Services mandates. This explains why certain industries (healthcare, financial) are heavily represented in breach lists. But many other industries no doubt experience breaches that go unreported. In Affinity's case, the breach occurred when a digital copier was returned to a warehouse without hard disk erasure – a leak point that many companies could easily overlook.

409,000

9. WellPoint/Anthem BlueCross: High-tech threats have headline appeal, but many breaches result from old-fashioned hacks like URL manipulation. For example, according to a lawsuit filed by the state of Indiana, WellPoint/Anthem failed to implement security precautions when it upgraded authentication code on the company's insurance application website. As a result, altered URLs could have been used to access personal data for up to 470,000 applicants, who were not notified until three months after the issue was found. Delayed notification adds insult to injury; stats demonstrate much room for improvement.

8. CitiGroup: Ultimately, many breaches are still the result of human over-sight or error. For example, approximately 600,000 CitiGroup were sent annual tax documents that had Social Security numbers printed on the outside of the envelope. Even though these SSNs were printed in a way that resembled mail routing numbers and may not have resulted in actual identity thefts, this shows how even a highly-regulated company with rigorous data handling processes can still shoot itself in the foot in a fairly big way.

7. Ohio State University: Roughly 10 percent of 2010 breaches involved educational institutions, such as this one reported by OSU. In late October, the university discovered suspicious activity on a server that stored the names, SSNs, birth dates, and addresses of up to 760,000 current and former students, faculty, staff, consultants and contractors. According to OSU, investigation confirmed unauthorized access but did not find evidence of data theft. Rather, hackers are believed to have used the server to launch attacks against other businesses. So why this breach notification? Most likely, the data housed on this server was not protected by encryption. (If records have been encrypted, ITRC would have indicated that no data was believed to have been exposed.)

6. South Shore Hospital: By now, you'd think that lost tapes would be a distant memory – not at South Shore, which lost up to 800,000 records containing personal, health and financial data associated with volunteers, patients, vendors, business partners and employees. The affected tapes were retired and being destroyed by Archive Data Solutions (formerly Iron Mountain) when that disposal was subcontracted to a geographically distant firm and three boxes of tapes were lost in transit. The moral: Safe destruction of old data is just as important as safe storage of current data.

5. Lincoln National Financial Securities: Password management counts. Not only did Lincoln National mistakenly *print* a username and password in a brochure posted on a public website, but it let employees and affiliates share usernames and passwords. Unfortunately, those credentials belonged to a portfolio information system housing data for 1.2 million customers. This single incident accounts for nearly all of the records breached by insider access during 2010 – but most other insider breaches were reported as having unknown record impact. According to the ITRC, just 51 percent of all breaches report number of records exposed, making it hard to assess their severity.

Related Articles

- Top 10 Mobile Mistakes to Avoid This Holiday Season
- 10 Ways to Protect Yourself from Firesheep Attacks
- Top Ten Ways to Avoid an Evil Twin Attack
- Ohio State Deals With Massive Data Breach
- Honda Acknowledges Security Breach
- California Agency Acknowledges Security Lapse

4. AvMed Health Plans: Two laptops were reportedly stolen from AvMed corporate offices in February 2010. Upon investigation, it was found that one laptop may not have been protected properly, putting current and former subscribers and their dependents at risk for identity theft. This breach was first estimated at 200,000 records then revised to 1.2 million. This case is an excellent illustration for the value of laptop encryption – and the ability to provide proof thereof. In fact, nearly 7 million records were breached last year due to lost, stolen, or discarded portable devices.

3. Gawker: In December, Gawker's database was hacked by Gnosis, exposing up to 1.3 million user email addresses and passwords. Not only were over 250,000 cracked passwords posted on on-line, but Gnosis published a link to Gawker's entire MD5 hashed password database. Shortly thereafter, HD Moore posted instructions on how to check whether any password was included in the posted database, and stats emerged about commonly used passwords. (The winner: "123456") Although no SSNs or financial data were specifically breached in this case, impact could be far broader due to the common practice of user login reuse across websites.

2. Educational Credit Management Corp: Safes stolen from this student loan firm contained portable media used to store personally identifiable information corresponding to 3.3 million people. These stolen items were actually recovered shortly after the theft but spent weeks in a police evidence room before being discovered. What can we learn from this breach? Avoid relying on physical security alone – there can be little excuse now that portable media data encryption is so readily available.

Finally, first place on our 2010 breach list goes to...

1. Netflix: According a class action suit filed in January 2010, Netflix "perpetrated the largest voluntary privacy breach to date" when it supplied data sets containing over 100 million subscriber movie ratings and preferences to contest participants.

Netflix argues that the data sets were anonymized and did not contain subscriber names or other personal information. However, the suit alleges that researchers have been able to crack Netflix's anonymization process to identify individual subscribers.

ITRC does not consider this incident to be a breach due to the nature of the records involved. However, the Privacy Rights Clearinghouse does. This incident demonstrates that sensitive personal data comes in many forms. Victims may have different perspectives on risk; this further complicates breach reporting.

So what can we learn from this year's list? Surprisingly few of these big breaches are associated with trendy new technologies. Instead, many can be attributed to either old fashioned hacks, basic omissions in security best practices, or errors in security policies and processes. Case in point: Paper breaches account for nearly 20 percent of this year's complete list. When you hear hoof beats, think horses, not zebras.

New technologies offer opportunities to build data security into networks, devices, and applications from the very start. But we still need to get those old familiar security fundamentals right to avoid data breaches and exposures – reported or otherwise.

Lisa Phifer owns Core Competence, a consulting firm focused on business use of emerging network and security technologies. Since 1997, Lisa has been involved in mobile workforce policy development and best practices, ranging from wireless/VPN security to portable data defenses.

Keep up with security news; Follow eSecurityPlanet on Twitter: @eSecurityP.