


 SQL Server 2005

 Microsoft®
SQL Server 2005

Corporate Sloppiness Is the Real Culprit for Data Loss, Not Vilified Hackers

March 28, 2007

By Lisa Vaas

Expect to see the 2 billionth personal record compromised by year's end, according to recent research from the University of Washington. But don't blame it on rogue hackers; sorry to say, it's your own fault, Corporate America.

Researchers at the university in Seattle estimate that electronic records—those containing Social Security or credit card numbers, academic grades or medical history—are bleeding out of North American organizations at the rate of 6 million a month so far in 2007—up some 200,000 a month from last year.

ADVERTISEMENT



Excluding the exceptional 2003 incident that involved 1.6 billion records stolen from information aggregator Acxiom, hackers have been responsible for only about 550—31 percent—of confirmed breaches between 1980 and 2006.

RELATED LINKS

[RFID Feared as Possible Terrorist Target](#)

[The Now-What of Losing Customer Data](#)

[We're Number One! ... For Malicious Internet Activity](#)

[Report: Government Domains Safe—Unless It's Romania](#)

[Report: Some Companies Lose Data Six Times a Year](#)

The majority, 60 percent, of incidents of compromised records were attributed to organizational mismanagement. That includes missing or stolen hardware, administrative errors, insider abuse or

theft or accidental posting of sensitive information online. The balance of 9 percent of breaches were due to unspecified circumstances. Even with Axiom removed from the picture, the commercial sector still accounts for about 252 million individual compromised records, four times that of the next-highest contributor, the government.

[The laptop is lost. Now what? Click here](#) to find out.

In order to examine the role of organizations' behavior in privacy violations, two UW researchers analyzed 589 incidents of compromised data between 1980 and 2006 by collecting news accounts out of major U.S. news media outlets including the New York Times and USA Today.

The researchers were Phil Howard, an assistant professor of communication, and Kris Erickson, a UW geography doctoral student. Their report, titled "[A Case of Mistaken Identity? News Accounts of Hacker and Organizational Responsibility for Compromised Digital Records, 1980–2006](#)," delves into the flood of escaping records and some of the related dynamics and is due to appear in the July edition of the [Journal of Computer-Mediated Communication](#).

The authors say that organizations can probably be blamed for the management practices that result in administrative errors, lost backup tapes or data exposed online. Organizations aren't off the hook just because of a data compromise caused by an insider, though. "Even though an organization can be the victim of theft by its employees, we might still expect organizations to develop suitable safeguards to ensure the safety of client, customer or member data," the authors write.

In a press release, UW said that Howard and Erickson were careful to avoid double counting press accounts of the same breached-record incident that led to exposed credit histories and other personal information. In fact, Howard writes in the report that the researchers' numbers likely underestimate the number of data breaches pre-2003, when California's pioneering [Security Breach Information Act \(SB 1386\)](#) took effect. That law requires companies to disclose security lapses. More than 20 states have since adopted statutes modeled on California's.

During their analysis, Howard and Erickson also found that SB 1386 and similar legislation is likely responsible for the number of reported incidents more than tripling in 2005 and 2006 compared with the previous 24 years, given that such legislation wasn't widely adopted until 2005.

Besides the fact that laws are forcing organizations to report data breaches, another factor in the sharp increase in incidents since 2005 is likely the fact that institutions are maintaining a larger quantity of electronic data. Another possible cause of the spike in electronic record loss, and the one its authors found most plausible, is that the mandatory reporting legislation has exposed both the severity of the problem and the frequency of organizational mismanagement.

The increasingly harsh punishments meted out to illegal hacking has actually allowed commercial, educational, government, medical and military organizations to avoid being held responsible for their lax attention to data security, the authors claim.

How to turn the situation around is another question entirely. The report suggests alternatives such as setting stricter standards for information management, levying fines against institutions that violate information security standards and mandating the encryption of all computerized personal data.

There are problems with such approaches, however. "The introduction of legislation to directly regulate institutions that handle electronic information would certainly be controversial," the report notes. "A wide variety of agencies, companies and organizations manage personal records on a daily basis. This complexity would hinder the imposition of standardized practices such as encryption protocols. Corporations would probably balk at the prospect of having to pay fines or introduce expensive security measures and accuse the government of heavy-handed interference. Others might argue that the imperatives of free-market capitalism demand that the government refrain from adopting punitive legislation, especially in order to maximize competitiveness."

Check out eWEEK.com's Security Center for the latest security news, reviews and analysis. And for insights on security coverage around the Web, take a look at [eWEEK's Security Watch blog](#).

Copyright (c) 2007 Ziff Davis Media Inc. All Rights Reserved.