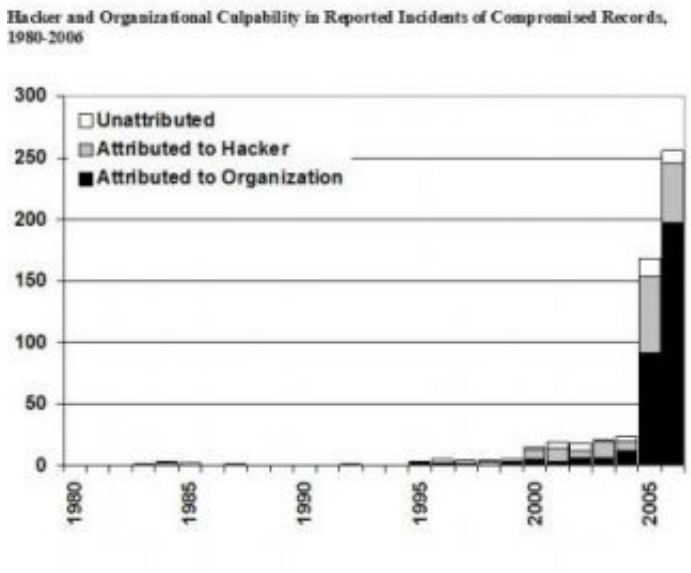
Hackers get bum rap for corporate America's digital delinquency

March 13 2007



Hacker and organizational culpability in reported incidents of compromised data 1980-2006. Credit: Phil Howard

If Phil Howard's calculations prove true, by year's end the 2 billionth personal record – some American's social-security or credit-card number, academic grades or medical history – will become compromised, and it's corporate America, not rogue hackers, who are primarily to blame. By his reckoning, electronic records in the United States are bleeding at the rate of 6 million a month in 2007, up some 200,000 a month from last year.

Howard, an assistant professor of communication at the University of Washington, bases his projections on a review of breached-record incidents as reported in major U.S. news media from 1980 to 2006. The total through last year stood at 1.9 billion – or roughly nine records per American adult.

His report delving into the flood of escaping records and some of the related dynamics, co-authored with Kris Erickson, a UW geography doctoral student, will appear in the July edition of the Journal of Computer-Mediated Communication. If anything, Howard contends the numbers they collected are conservative.

He said they were careful to avoid double counting press accounts of the same breached-record incident that led to exposed credit histories and other personal information. He believes similar incidents took place, but went un- or underreported before 2003, when California's pioneering Notice of Security Breach law took effect. That law requires companies to disclose such lapses, and more than 20 states, including Washington, have since adopted statutes modeled on California's, Howard said.

He and Erickson also found that:

-- Malicious intrusions by hackers make up a minority (31 percent) of 550 confirmed incidents between 1980 and 2006; 60 percent were attributable to organizational mismanagement such as missing or stolen hardware; the balance of 9 percent was due to unspecified breaches.
-- Likely as a result of California's law and similar legislation adopted by other states, the number of reported incidents more than tripled in 2005 and 2006 (424 cases) compared to the previous 24 years (126 cases).
-- The education sector, primarily colleges and universities, amounted to less than 1 percent of all lost records, but accounted for 30 percent of all reported incidents.

A single 2003 incident involving 1.6 billion records held by Acxiom, an Arkansas-based company that stores personal, financial and corporate data, dwarfs all others. In that case, the offender controlled a company that did business with Acxiom and had permission to access some files on Acxiom's servers. But he illegally hacked into other records and then tried to conceal the theft, prosecutors charged.

A much different picture emerges, however, when the past quarter century is viewed in terms of the number of reported incidents. Three out of five point to organizational malfeasance of some variety, including missing or stolen hardware, insider abuse or theft, administrative error, or accidentally exposing data online, Howard and Erickson found.

Thanks to the mandatory reporting process established by California, "We've actually been able to get a much better snapshot of the spectrum of privacy violations," Howard said. "And the surprising part is how much of those violations are organizationally prompted – they're not about lone wolf hackers doing their thing with malicious intent."

While corporate America would prefer to let "market forces" – factors such as negative publicity and expenses generated by data loss – take care of the problem the authors aren't convinced that would make for an effective strategy, especially with identity theft listed as the fastest-growing crime in the United States. Based on recent history, it looks as though states are more apt to fill the regulatory void than the federal government, Howard said.

Another noteworthy trend, he said, is what's happening in the education sector, which accounted for nearly a third of reported breaches. This could be explained, Howard and Erickson said, by the fact that colleges and universities "have an organizational culture geared towards information sharing."

Source: University of Washington