

Security experts: Hacking attacks rarely made public



Friday, February 18, 2005 Posted: 1:03 PM EST (1803 GMT)

WASHINGTON (Reuters) -- A security breach that placed consumers at risk for identity theft grabbed headlines this week but most hacking incidents go unreported to police or the public, experts said on Thursday.

Afraid of negative publicity, most companies that suffer intrusions take a tight-lipped approach that leaves consumers unaware when their identities may be compromised, they said.

At the same time, businesses are becoming more willing to discuss security issues with their competitors behind the scenes in an effort to head off online threats, an approach experts say has managed to reduce the impact of computer worms and viruses.

Still, a 2004 FBI cyber-crime survey found that only 20 percent of companies report computer intrusions to the police, and half don't report them to anybody.

"A business organization or a government organization for that matter has an obligation to inform the employees or customers that have been potentially harmed as a result of the data breach," said Larry Ponemon, a privacy and security consultant who has advised a wide variety of companies.

Only one state -- California -- requires companies to notify consumers when an outsider is able to access their Social Security numbers or other information that puts them at greater risk for identity theft.

Data-mining company ChoicePoint Inc. mailed out some 35,000 of those notices to California residents last week after it discovered that criminals had posed as legitimate businesses to access consumer dossiers it had compiled.

ChoicePoint will notify some 110,000 consumers outside California who may have been affected as well, company spokesman Chuck Jones said.

Privacy experts said the California law paradoxically may discourage companies from examining intrusions too closely for fear that they might have to make them public.

"There's a process in place that may be filtering out a lot of bad news," Ponemon said. "I really think that we have a problem here."

Jim Dempsey, executive director at the nonprofit Center for Democracy and Technology, said the issue might be better addressed by broad privacy legislation that outlines consumer rights rather than specific security requirements.

"How you structure responsibility is not an easily answered question, but it's one that Congress and the public and the industry needs to confront," he said.

Outside the public sphere, businesses have been more willing to discuss security issues, said Peter Allor, who oversees a cyber-security information center for the technology industry.

Though the center has been up and running since 2001, membership has spiked to around 60 since last summer, allowing members to block computer viruses before they can cause major damage, he said.

"You can actually go and work with competitors and with partners and discuss information in a protected manner," he said.