c|net NEWS.COM http://www.news.com/

Feds scramble to meet data breach deadline

By Anne Broache
http://news.com.com/Feds+scramble+to+meet+data+breach+deadline/2100-7348_3-6197474.html

Story last modified Mon Jul 23 12:08:30 PDT 2007

A correction was made to this story. Read below for details.

WASHINGTON--With only two months left before government agencies must figure out how to deal with data breaches and data theft, federal bureaucrats are scrambling to meet the looming deadline.

The deadline was created by a White House directive (PDF) published this spring that gave all federal agencies until September 22 to figure out the wisest way, using their "best judgment," to come up with a plan to secure Americans' personal data and to alert them if it falls into the wrong hands.

Finishing everything by that date is "definitely a challenge," Mischel Kwon, chief IT security technologist for the U.S. Department of Justice, said Wednesday.

The White House's order appears to have been prompted by a rash of computer security foibles at federal agencies in recent years, including the high-profile theft last year of a laptop and hard drive containing data on 26.5 million past and present military personnel.

Although Congress has been weighing legislation that would prescribe new requirements for government agencies and businesses that suspect or discover security intrusions, one supporter of a new such law said Wednesday that it might be better to wait and see if everyone does a good job of meeting the September 22 deadline.

"I don't like being overly prescriptive," Rep. Tom Davis (R-Va.) told an audience of about 250 representatives from various federal and state government agencies attending a briefing organized by the *Homeland Defense Journal*. "If we allow them to do their job and give them appropriate training, they can do a better job than we can in Congress."

"From a security point of view, the biggest challenge with this directive is actually doing security."

--Mischel Kwon
Department of Justice

While it's not clear how effective a set of written policies will be if they're not always followed and not part of the culture of an existing agency, the White House memo does recommend techniques such as encryption, limiting remote access and access logging. At the very least, the memo says, egregious disregard of privacy safeguards would result in an employee's "prompt removal of authority to access information."

The chief privacy officers for the U.S. Department of Homeland Security and the Federal Trade Commission said they were in the process of taking steps to comply with the White House order. Homeland Security's Hugo Teufel said he sent a memo on Tuesday to top officials within the department outlining what its plans would be, although he did not describe them at Wednesday's session.

The FTC's chief privacy officer, Marc Groman, said his agency had prepared a 12-page compliance plan last month. He showed the audience a slide with the document's table of contents, which covered topics including notifying third parties, notifying individuals and identity theft risk analysis. The FTC has also set up a Breach Notification Response Team composed of high-level officials from throughout the agency who would be charged with meeting "immediately" to do an initial evaluation of a breach report and to decide what to do next.

But some officials speaking at the briefing session cautioned against relying too heavily on abstract policies alone.

"From a security point of view, the biggest challenge with this directive is actually doing security," said the Justice Department's Kwon. "I don't think security is addressing bullets in a memo; I think it's evaluation and risk assessment, and sometimes it's more and sometimes it's less than the bullets on the page."

A common thread among the presentations was that of building flexibility into the written policies--and to work hard at making sure employees and contractors at every level actually know about and understand what to do.

"Whenever you have humans or carbon-based forms, they make mistakes, so you have to train, train, train," Homeland Security's Teufel said.

The FTC's Groman urged the audience to do more than merely draft policy statements. In March, the trade agency held a weeklong privacy summit for its employees, devoting one mandatory "clean-up day" to forcing everyone, clad in jeans and T-shirts--if they wished--to take inventory of all of the sensitive or personally identifiable information they had in their possession (including in their cubicles or on their computers).

Now on News.com
Xbox repairs leave gamers in a fix Perspective: Bulls, bears and BS All the news that's fit to link Extra: Lax computer security at IRS

The agency plans to stage a similar event later this year focused on protecting agency data. It has already started drafting posters bearing questions like, "You left your FTC BlackBerry on the Metro--What do you do?" The unsurprising answer at the bottom: "Tell your manager."

Others on the panel encouraged federal agencies to think rationally about their plans for protecting data in the first place. Many agencies, for instance, are tempted to adopt a blanket practice of hard drive encryption on their machines. But that isn't necessarily the wisest option because it's only effective if a computer isn't already booted up, warned the Justice Department's Kwon and Tim Grance, manager of systems and network security for the National Institute of Standards and Technology (NIST). They said it's important to tailor different levels of protection to the type of data being shielded.

Besides, any form of encryption "doesn't do a lot of good if you're not going to use keys properly," Grance said. "It's not going to do you a lot of good if you use your e-mail password for the encryption key...That's high on my list of dumb things to do."

Correction: This story misidentified the publication that hosted a briefing on data breach prevention, mitigation and notification. It is the *Homeland Defense Journal*.