Security
April 14, 2009 10:57 AM PDT

Why a national data breach notification law makes sense

by Jon Oltsik

Font size
Print
E-mail
Share

Yahoo! Buzz

As we await the **60-day federal cybersecurity review from Melissa Hathaway**, acting senior director for cyberspace for the National Security and Homeland Security Councils , there is something else that could be done. It seems to me that the federal government could take another related action to help protect the private information of U.S. citizens while reducing the cost of doing so. In my humble opinion, it is time to create a single federal data breach disclosure law. I believe this action would:

1. **Simplify the maze of current state legislation**. As of the end of December, 44 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted security breach notification legislation. While most of these laws are modeled on the **original California legislation (SB-1386)** that took effect in 2003, there are subtle differences in terms of deadlines for notifications, definitions, and civil penalties. Massachusetts and Nevada have gone the furthest so far by mandating that private data be encrypted in certain circumstances. Obviously, this creates a legislative mess that could be streamlined by one central federal regulation.

2. **Protect the unprotected**. In the six years since California started the trend toward data breach notification legislation, Alabama, Kentucky, Mississippi, New Mexico, and South Dakota have no such laws in place or have laws that haven't taken effect. I'm not sure why this is but citizens in these states deserve the same type of protection we others have.

3. **Extend the definition of private data into other areas**. Aside from state

> data notification laws, many large organizations must still comply with the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, Sarbanes-Oxley Act, etc. There must be a way to broaden the definition of private data and consolidate private data security and breach notification legislation like the European Union has. The cost of compliance could go down precipitously if organizations were not obligated to perform the same basic tasks and audits numerous times.

If we are truly looking for ways to improve electronic data security *and* reduce cost and overhead, this seems like a good plan to me. I know my argument is simple and I'd be glad to learn more as to whether this logic makes sense. Please let me know if my instincts are correct or whether I've missed some important issues.

Jon Oltsik is a senior analyst at the Enterprise Strategy Group. He is not an employee of CNET.

Topics: **Privacy & data protection**

Tags: **federal data breach disclosure law**, **data breach notification**, **cybersecurity review**

Share: Digg Del.icio.us Reddit Yahoo! Buzz

Related

From CNET

The marriage of identity yin and security yang

AT&T Wireless has surprising new terms of service

On the security road to 'de-perimeterization'

From around the web

Utimaco Partners with Ropes and Gray, So... AOL News

Gadgetwise: Samsung Makes an Impression ... The New York Times