FEATURE

Data breach notification laws, state and federal

A review with commentary for security C-Levels

By David Geer
CSO |
NOV 1, 2013 7:00 AM PST

State and federal data breach notification laws have changed and are expanding more than a little bit. CISOs and CSOs should start here to expand their knowledge of the increasingly restrictive notification requirements that apply to their organizations.

State Law Status and Trends

One challenge enterprises have faced with state data breach notification laws is the differences between the laws. "When you have an incident that affects consumers throughout the country, you have to craft a response that complies with all the state laws, which is a challenge. It's even impossible where there's an outright contradiction between two different laws," says Kristen J. Mathews, Partner, Privacy & Data Security Group, Proskauer Rose LLP.

[Learn 8 pitfalls that undermine security program success and 12 tips for effectively presenting cybersecurity to the board. | Sign up for CSO newsletters.]

While Massachusetts' breach notification law says the letter the company sends to affected individuals cannot inform as to the nature of the breach, most states require the opposite. "The only way to comply is to have a special letter for Massachusetts. In that letter, you delete the information about the nature of the breach," says Mathews.

A new challenge is states' broadening definitions of the personally identifiable information (PII) or protected health information (PHI) that triggers notifications. "While most states cover social security numbers, driver's license numbers and financial account numbers, we're seeing states add pieces to their definitions like health information, health insurance information and passwords," says Mathews. California's breach notification law now includes the username

and password combinations for online accounts in its list of PII/PHI, notes Mathews. Such login data for any online account would qualify. Ultimately, there will be many more instances in which enterprises will have to notify.

[Lawmakers push for federal data breach notification law]

State laws are also increasingly requiring companies to notify their attorneys general. "If you have a breach, you have to notify consumers, but you also have to send a letter to the state attorney general. AGs review these notices and can decide to launch investigations of companies to see whether there was any wrong doing on their part that caused the incident," Mathews says.

But, perhaps the most disconcerting to enterprises is the state-level trending toward including deadlines for notifying affected consumers. "A lot of states are adding timing restrictions in the form of a number of days," says Mathews. For example, Florida now has a 45-day time limit. This can easily put companies in the position where they may not have concluded the research necessary to determine whether they must notify before the notification must go out.

Federal Law Status and Trends

In the new HIPAA Omnibus Final Rule effected September 23rd of this year, the federal government has made data breach notification requirements more restrictive. "The law used to say that you have to notify the patient if the incident poses a significant risk of financial, reputational or other harm to the individual," says Mathews. That is what the industry calls a risk of harm threshold. The law now states that you have to notify in all situations except those in which there is a low probability that the breach compromised the individual's information, Mathews clarifies. "With the new standard, it is even harder to avoid notifying your customers," says Mathews.

[Privacy commissioner backs mandatory data breach notification]

"The HIPAA Omnibus Final Rule says you have to do a risk assessment on every PHI breach," says Scott Pettigrew, CSO, HMS Holdings Corp. The rule offers four criteria that enterprises must use to perform that assessment. According to Pettigrew, the criteria include the nature and extent of the PHI involved and the likelihood of re-identification of the individual; the identity/role of the authorized person who used the PHI; whether an unauthorized person acquired or viewed the PHI; and the extent of the mitigation of the risk to the PHI.

The HIPAA Omnibus Final Rule establishes other requirements. A business associate or contractor who handles data with PII/PHI, such as when performing data processing on behalf of the enterprise must now also notify in case of a breach where someone could trace the compromised data back to the affected individual.

"The Omnibus Rule requires more stringent oversight by Health and Human Services (HHS). With every breach notification that affects more than 500 people, HHS must launch an investigation," says Pettigrew. Organizations will have to have proof that they performed a risk assessment. They will have to stand by any risk assessment results that lead them to withhold notification, explains Pettigrew.

The rule also bridles the state laws, permitting the more stringent ones to apply only as long as they are not contradictory to the federal law. Enterprises must update their procedures and train their workforces on all the new breach rules to satisfy the Omnibus Rule.

The Future of Data Breach Notification

A single federal law applicable to all PII/PHI would seem to benefit enterprises. Congress has been writing and circulating bills for years that would accomplish something like this. "Most of those bills would preempt the state laws, which would be very good for businesses because we wouldn't have to look at those state laws anymore. We would only have to follow one federal law to craft a notification," says Mathews. Unfortunately, congress is not passing these bills yet.

[Encryption would exempt ISPs from data breach notification to EU customers]

To stay abreast of state laws, a quick search on Google for "data breach chart" or "data breach notification chart" will return links to charts and indexes of state notification laws, including some hosted on attorneys' professional websites. For federal laws, look to HIPAA/HITECH and the HIPAA Omnibus Final Rule. For actual breaches, keep the appropriate attorney/privacy expert on speed dial.

Next read this

- *The 10 most powerful cybersecurity companies*
- *7 hot cybersecurity trends (and 2 going cold)*
- *The Apache Log4j vulnerabilities: A timeline*
- *Using the NIST Cybersecurity Framework to address organizational risk*
- *11 penetration testing tools the pros use*

7 hot cybersecurity trends (and 2 going cold)