Data protection

Solid state

ebook

An SC Magazine publication

Sponsored by

Solid state

A new privacy regulation in Massachusetts evokes anxiety for many, but getting in line may prove to be no big deal, reports Greg Masters.

After a few delays, what has been termed the nation's strictest state data security regulation is set to go into effect on March 1 in Massachusetts. The legislation, 201 CMR 17.00, details a number of requirements that all companies, no matter where they are based, must follow to safeguard the paper or electronic records in their possession of any Massachusetts resident.

Businesses that possess personally identifiable information (PII) of Bay State residents will now be required to encrypt all devices and transmissions. In addition, businesses must have an employee dedicated to security efforts, restrict access to company data to only those employees requiring access, regularly monitor enterprise security programs, and develop, implement and maintain a "comprehensive information security program."

The Massachusetts legislation goes further than most data security regulations by prescribing specific technical measures that must be taken to protect PII, says Boaz Gelbord, executive director of information security at a New York-based company that assists educators and students. It's the legislation's degree of specificity, he says, that distinguishes it from the generic language typical in such regulations.

"In most regulations, you have to maintain confidentiality, but you don't see references to specific technology," Gelbord says.

Also, this legislation differs from other state disclosure bills because it forces businesses to become proactive in securing technology, says Gretchen Hellman, vice president of security solutions for Vormetric, a data security solutions provider. It insists that organizations take measures to protect information, as opposed to other guidelines that only require companies alert customers should their data be compromised, she says.

In short, the Massachusetts bill puts together requirements to prevent breaches from happening in the first place, she says.

Robbie Higgins, vice president for security services at GlassHouse, a global provider of IT services, adds that, in most cases, the regulation lays out what any business should already be doing as far as security goes. "It may be a little heavy in certain areas, like encryption, but it makes sense," he says.

Higgins sees one of the bill's primary challenges for companies as identifying exactly where its information resides. "Once they determine where the PII is – whether it's on a disk or email – then they can address it."

But, he warns, some companies don't understand where the data is, while others mistakenly believe they need to encrypt everything. Another big challenge is figuring out what percentage of employees deal with this information.When it comes down to it, though, Higgins says this regulation is not going to address all security concerns.

"It's not a roadmap for security in the business environment, it's more a guideline," he says. "Yes, you need to make sure to comply, but that in itself is not a security blueprint if you're looking to properly secure your environment."

Many businesses have been following HIPAA and PCI mandates, but that has not been enough to prevent major data breaches, he points out.

"As things become more distributed, determining where data is and how much access and control a business has brings challenges," he says. Virtualization, for example, depends on hosting data with a third party. Is this site multi-tenanted, he asks. It can be difficult to audit against.

Easing regulation anxiety

When strict data breach security regulations were first proposed in Massachusetts around two years ago, IT leaders at a lot of small

450

cases of lost or stolen information has impacted some 700,000 Massachusetts residents since 2007

businesses were anxious, says Jim Lippie, president of Staples Network Services by Thrive, an outsourced IT provider based in Lawrence, Mass. But, as the company began working with clients, Lippie found that the regulation is not, in his words, that big a deal, particularly for those companies that adhere to industry best practices. By this he means health care businesses already toeing the compliance line owing to HIPAA mandates, or enterprises that process credit cards already governed by PCI guidance. "They have the right procedures in place," he says.

One example he points to is a large insurance company that contacted his team when the regulation was announced. "They were very anxious, but after an initial assessment, it only took a few fixes."

Technology specifics

"The regulation does much better when it advises on procedural issues more than the technical issues," Gelbord says. The trend in these types of laws, he says, is to avoid specific requirements for technology as these can quickly become out of date. "The government is not the best place to dictate technology matters," he says.

Specifically, Gelbord cites the law's narrow focus on anti-virus software, operating system security patches, firewalls and encryption. The problem is that these traditional security measures are not sufficient to address the threat posed by web-facing application vulnerabilities. The weakness in the regulation is not focusing enough on higher risk issues, he says.

"It's behind the times in the kinds of threats it seeks to address. It focuses on network security and anti-virus while ignoring the risk posed by web application vulnerabilities, like SQL injection. In today's internet, proper input validation for a web application is just as important as maintaining up-to-date virus definitions when it comes to protecting PII," Gelbord says.

And, while language in the document has been altered in response to criticism, there are still some concerns. The definition of encryption was too specific in the original version, says Nagraj Seshadri, senior product marketing manager, Sophos. The mandate's original definition of encryption has since been modified, changing from an "algorithmic" process to a "confidential" one.

Further, Seshadri points out that there is too much ambiguity with the phrase "to the extent technically feasible," applied to the implementation of the list of technical requirements. It places a responsibility on the businesses to determine what is, in fact, technically feasible.

"From a technologist's point of view, all the technologies listed in the requirements are available today, so if companies choose not to implement certain technologies, they should have a very good reasoning behind it in case they are called to defend their position," Seshadri says.

Mom-and-pop shops

Another part of the law that's unclear is just how much leeway small companies will have when it comes to implementing the technical safeguard requirements, says Gelbord. Some of the requirements could prove costly for small businesses that do not have enterprise-grade IT systems in place, but the regulation contains language that appears to weaken the requirements for SMBs.

Further, while bigger enterprises are likely already in line with the state's provisions from following other laws, for mom-and-pop shops, it's a big deal to secure their business, says Vormetric's Hellman.

Sophos's Seshadri agrees. He says that one of the biggest concerns about the initial versions of the regulation was that it followed a one-size-fits-all approach regardless of the size or scope of the business and the amount of data stored.

"It was felt that this placed undue burden – in terms of resources, cost and required

71%

of companies said they don't encrypt data on laptops

– Novell study

expertise – on smaller businesses because they would be held up to the same standards as large businesses," says Seshadri

"The requirement to take a risk-based compliance approach to data protection takes several factors into account, including the size and scope of business, the amount of data that is captured or stored, the resources available to the company and the level of security expected based on the nature of the business. Smaller businesses could use this approach to consolidate technologies and deploy more manageable and cost-effective solutions," he says.

He adds that the initial version of the regulation that required businesses to review and possibly rewrite all their contracts was a practically impossible exercise. "As a result, in the amended regulations, the requirement for third parties to secure personal information has been changed to be consistent with federal data protection laws wherever applicable," he says.

Businesses are now expected to take reasonable steps to ensure that third parties take appropriate security measures. "The regulation's revisions also recognize that businesses may have prior contracts with third parties, so it is important to businesses to re-read the fine print and dates in their contracts to ensure that they stay compliant."

Wait and see

It will take time to decide whether the regulation is a good model, says Vormetric's Hellman. "It's hard to regulate good security. Security is a consistent effort. Regulations will always fall short. It's impossible to put together a regulation that applies to all companies and says this is what makes you secure."

By and large, though, says executive director Gelbord, most companies with reasonable security measures in place, should be in good shape. "It will be interesting to see whether this law will be replicated by other states in the future, whether this will prove to be a model going forward, and to see what actions are taken as a result," he says.

For its part, Staples Network Services has assembled a 26-point matrix it uses as a compliance checklist to determine what clients must do to meet security requirements. Taking it further, Lippie says the company has put together pieces of legislation from all over the globe to have the most stringent privacy protection plan in place.

"Once we take the time to understand what the policy is, it shouldn't be overwhelming," says Lippie. "It isn't the huge change that people once thought it would be."

However, questions remain about how 201 CMR 17.00 will be enforced. Unless there's a breach, there's no way to determine whether a company is following the guidelines, says Lippie.

Nevertheless, for most businesses in Massachusetts the regulation should have no effect, GlassHouse's Higgins says. "They should have these systems in place. For most companies, it should be fairly straightforward. If companies implement security controls and follow industry best practices for a good security program, they shouldn't run into any challenges," he says, adding that only time will tell whether the mandates have any real impact. ■

1,000

laptops a week are left at airports

–Ponemon Institute

Sponsor

Thawte is a leading global Certification Authority. Our SSL and code signing digital certificates are used globally to secure servers, provide data encryption, authenticate users, protect privacy and assure online identifies through stringent authentication and verification processes. Our SSL certificates include Wildcard SSL Certificates, SGC SuperCerts and Extended Validation SSL Certificates.

Masthead

EDITORIAL

EDITOR-IN-CHIEF Illena Armstrong
illena.armstrong@haymarketmedia.com

MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com

DESIGN AND PRODUCTION

ART DIRECTOR Brian Jackson
brian.jackson@haymarketmedia.com

SENIOR PRODUCTION/DIGITAL CONTROLLER
Krassi Varbanov
krassi.varbanov@haymarketmedia.com

U.S. SALES

ASSOCIATE PUBLISHER, VP OF SALES Gill Torren
(646) 638-6008 *gill.torren@haymarketmedia.com*

EASTERN REGION SALES MANAGER Mike Shemesh
(646) 638-6016 *mike.shemesh@haymarketmedia.com*

WESTERN REGION SALES MANAGER Matthew Allington
(415) 346-6460 *matthew.allington@haymarketmedia.com*

NATIONAL INSIDE SALES EXEC. Brittany Thompson
(646) 638-6152 *brittany.thompson@haymarketmedia.com*