Up to code

An insurance company found help getting into compliance with a strict data law.

ebook

An SC Magazine publication

Sponsored by

thawte®

tripwire™

Up to code

An insurance provider in Massachusetts had basic security measures in place, but these were not enough to be fully compliant with a strict, new state regulation, reports Greg Masters.

When Massachusetts passed what arguably is one of the most stringent data protection laws in the nation last March, Ray Pata, the manager of systems and programming at A.I.M. Mutual Insurance Cos., found himself particularly challenged with the encryption of laptops, required by the new law.

The legislation, 201 CMR 17.00, requires that all companies, no matter where they are based, must 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.

This legislation differentiates itself from other state disclosure bills because it forces businesses to become proactive in securing technology, insisting that organizations take measures to protect information, as opposed to other guidelines that only require companies alert customers should their data be compromised. In addition, it requires that businesses restrict access to company data to only those employees requiring access, have an employee dedicated to security efforts, regularly monitor enterprise security programs, and develop, implement and maintain a "comprehensive information security program.

While A.I.M. Mutual Insurance Cos. already had several basic security measures in place, such as anti-virus, firewalls, etc., these were not enough for the provider of worker's compensation in Massachusetts to be fully compliant with the new state regulation. The company is headquartered in Burlington, Mass., and also has satellite offices throughout the state, and in neighboring New Hampshire.

To upgrade the company's defenses in order to bring it up to compliance with the new state requirement, Pata and his team – comprised of three developers and a network specialist – began a review of the standard offerings available. After an assessment and trial period, they chose a solution from BitArmor, recently acquired by Trustwave.

"As a small organization, deploying encryption can be hard, and this could have been a challenge for us. However, BitArmor Managed Encryption made it easy for us to be compliant."

AIM uses BitArmor Managed Encryption across the internet to manage its encryption environment, after software has been deployed on vulnerable laptops in the company, says Patrick McGregor, CEO of BitArmor. The tool provides a single integrated solution for full-disk encryption, USB encryption and email attachment encryption.

"This enables the customer to protect the most vulnerable points in their environment and helps them to be compliant with state data privacy laws and federal regulations, such as *HIPAA*," McGregor says.

> "Deploying encryption can be hard, and this could have been a challenge for us..."
>
> *– Ray Pata, manager of systems and programming, A.I.M. Mutual Insurance Cos.*

Most vendors, he points out, can't service small- and mid-sized organizations since they require dedicated management servers to be installed , which are managed inside the company. Or, if they provide a service from the cloud, they do not have multitenant server capabilities that completely and cryptographically separate one customer from another.

"Multitenancy is critical for solid data security and it provides economies of scale," says McGregor. The lack of such a multitenant architecture will increase costs and therefore will not be affordable for smaller organizations."

93%

of companies that lost their data center for 10 days or more due to a disaster, filed for bankruptcy within one year of the disaster.

– National Archives & Records Administration

McGregor also points out that it is often the case that key management and configuration are too complex for small organizations to address because they don't have dedicated security personnel.

"BitArmor Managed Encryption significantly reduces operational complexity – key management is automated, and because BitArmor hosts management servers in the cloud, the overhead of on-site hardware and maintenance is eliminated," he says.

And, data remains inside the organization, he adds. "All the encryption processing is done on customer devices and not in the cloud. This means that sensitive customer data never travels outside and customers have full control over their data at all times. BitArmor itself does not have any access to customer data."

Further, BitArmor Managed Encryption is very easy to manage, says McGregor. "Administrators do not need to be cryptographic experts – that is, there no need to manage, rotate, or revoke cryptographic keys."

> "This enables the customer to be compliant with state data privacy laws and federal regulations."
>
> *– Patrick McGregor, CEO of BitArmor*

Optionally, BitArmor can synchronize with the organization's Active Directory environment. This allows administrators to work with a familiar environment of users, groups and machines. Configurations are set centrally and trickle down to the end points. There is no need to touch individual endpoints to make changes.

Smooth deployment

Deployment of the BitArmor tool went very smoothly at A.I.M., says Pata. The vendor provided immediate resolution to any questions Pata and his team had. "Once we went through the first implementation of BitArmor's encryption on the first laptop, the remaining installations went quickly."

Tech tools: Secure sharing

Patrick McGregor, CEO of BitArmor, says BitArmor Managed Encryption provides:

Laptop encryption: The complete drive is encrypted and the organization can be assured that a lost or stolen laptop will not be compromised.

USB encryption: All data moving to a USB device will be automatically encrypted, thereby ensuring that users can transport document securely while ensuring its security.

Email attachment encryption: This enables organizations to have two-way secure sharing of encrypted data with partners – this ensures that data is always protected when it travels across public networks.

This was particularly important, he adds, because AIM has an obligation to provide the best means of protecting any personal information used in providing insurance services to its insureds.

"We especially liked the fact that we didn't have to maintain any additional hardware," he says. "BitArmor support was great to work with. Pricing was extremely competitive and it was quick to deploy," he says.

Right now, AIM is deploying the BitArmor tool to all of its laptops, says Pata. "We have road warriors that live and die by their laptops and because of the mobility, we want to ensure that these devices are fully protected."

He is pleased with the implementation because the encryption process is basically invisible to the users. "They have reported back to us that they experience no performance degradation as a result of installing the encryption product," he says.

And, when asked if he is finding it easy to manage and operate, he responds without hesitation, "Absolutely. Installation is quick,

25%

of all PC users suffer from data loss each year.

– Gartner

and with just a few clicks of the mouse, we can check the status of any and all the laptops."

The implementation is meeting his expectations. "We were looking for something that would be easy to install and maintain and not be a budget-buster," he says. "At the same time, we were looking to implement a level of security that would go beyond any regulatory requirements imposed on us."

Further, BitArmor's encryption product isn't just designed for laptops, he says, and the fact that the tool's encryption process can be applied to email attachments and USB devices has led him to look into expanding the installation to specific desktop PCs as well.

"The personnel at BitArmor have been great to work with," Pata says. "We haven't had much need to go to them with any issues, but whenever we've had a question, they've been very responsive. ■

For more information about SC Magazine ebooks, please contact Illena Armstrong, editor-in-chief, SC Magazine, *at illena.armstrong@haymarketmedia.com.*

77%

of companies which test their tape back-ups found back-up failures.

– Boston Computing Network

REDUCE COMPLIANCE CHALLENGES WITH TRIPWIRE SOLUTIONS

tripwire™
TAKE CONTROL.

The banking and financial services industry faces tremendous scrutiny by both domestic and international regulatory bodies. PCI, SOX, FFIEC and GLBA regulations and mandates aim to ensure the integrity of financial reporting information and the privacy and protection of personal information stored and transmitted in bank information systems.

It's a challenge to know where this data is stored and what controls are already in place to protect it. On top of that, ongoing risk assessments require that those controls be tested routinely. The challenge is further compounded by the complexity of the organizations in terms of the geographic distribution of offices, data centers and business units, the state of ongoing mergers and acquisitions, and the data-intensive business processes.

Tripwire solutions provide IT security and compliance automation to deliver intelligent change event management, enforce standards and policies, and remediate non-compliant configurations to protect valuable and sensitive data. Our comprehensive solutions help maintain a secure IT system by:

tripwire ENTERPRISE

tripwire LOG CENTER

- » Generating out-of-the-box policies for critical regulations and standards such as PCI, SOX, GLBA, FFIEC and SAS70.
- » Continuously addressing vulnerabilities one-by-one across the data center and virtual environments until the organization moves into a known and trusted state.
- » Providing dynamic change intelligence to prioritize changes or events of interest that cause you to drift out of compliance with built-in, real-time configuration control.
- » Instantly alerting you to all changes or suspicious events that could take you out of compliance.
- » Securely recording and generating reports representing current, historical and trend analysis of IT configuration changes and log events to enable audit preparedness.
- » Automating the repair of configurations that have fallen out of compliance and returning them to a secure and compliant state.

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.
For more information, visit www.thawte.com.

Headquartered in Portland, Ore., Tripwire has operations in 15 countries around the world. Tripwire's powerful IT security and compliance automation solutions help businesses and government agencies take control of their entire IT infrastructure.
For more information, visit www.tripwire.com.

Masthead

EDITORIAL
EDITOR-IN-CHIEF Illena Armstrong
illena.armstrong@haymarketmedia.com
DEPUTY EDITOR Dan Kaplan
dan.kaplan@haymarketmedia.com
MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com
DESIGN AND PRODUCTION
ART DIRECTOR Brian Jackson
brian.jackson@haymarketmedia.com
SENIOR PRODUCTION 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*