

INSIDE:

- 2 Moving Target
- 5 Identity Theft?
- 11 An Ounce of Prevention
- 18 Encrypt It or Else...
- 25 Get Ahead to Stay Ahead

THE MASSACHUSETTS DATA PROTECTION LAW

Massachusetts businesses facing down MA 201 CMR 17.00 can meet the challenge with preparation and execution.

MOVING TARGET

INTRODUCTION
MOVING TARGET

Keeping up with the Massachusetts data protection law may be more difficult than complying with it.

BY SCOT PETERSEN AND KELLEY DAMORE

CHAPTER 1
IDENTITY THEFT?



CHAPTER 2
AN OUNCE OF PREVENTION

CHAPTER 3
ENCRYPT IT OR ELSE...

CHAPTER 4
GET AHEAD TO STAY AHEAD

REGULATORY COMPLIANCE can be a challenging task for any corporation, but it can be particularly onerous if the regulation is a moving target.

This is the case of Massachusetts data protection regulation 201 CMR 17.00, which seemed ready to go into effect Jan. 1, 2010 (already delayed once from a May 2009 enforcement date). Just a few months ago, this state regulation was positioned as a game changer. It framed data privacy in a way that forced organizations to take steps to protect personal data. Today most state privacy laws focus on notifying people of a data breach rather than protecting the information in the first place. MA 201 CMR 17.00 was proactive, rather than reactive, security.

But due to the uncertain economy, costs associated with meeting the regulations and complaints from the

public, businesses and organizations, the Massachusetts Senate is now considering weakening the scope and specifics of the regulation.

The critical issues of encryption, jurisdiction and small business needs are at the heart of the proposed changes to 201 CMR 17.00, which put undo pressures on IT budgets and personnel, critics have charged. "The current regulations exceeded the intent of the legislature and are very problematic," says Anne Doherty Johnson, executive director of trade association TechAmerica New England, at the May 12 Senate hearing for the amendments.

CLIMATE FOR CHANGE

But in a legislatively aggressive climate such as we are in now, with new security exploits being discovered

INTRODUCTION
MOVING TARGET

CHAPTER 1
IDENTITY THEFT?

CHAPTER 2
AN OUNCE OF
PREVENTION

CHAPTER 3
ENCRYPT IT
OR ELSE...

CHAPTER 4
GET AHEAD TO
STAY AHEAD

every day and data breach disclosures such as those from The TJX Cos. and Heartland Payment Systems Inc., strict privacy and data protection laws from the state and federal levels

In a legislatively aggressive climate such as we are in now, with new security exploits being discovered every day, strict privacy and data protection laws are inevitable.

are inevitable. Simply stated, MA 201 CMR 17.00 is good security practice. So despite the near-term uncertainty about the particulars, the prudent move by corporate IT is to take steps now to be ready for tough encryption and policy statements later.

As we outline in this e-book, a joint effort of SearchCompliance.com and SearchSecurity.com, CIOs and senior IT managers all the way down to a sole proprietorship with no IT staff need to be aware of coming regulations, the technology and processes needed to secure privacy and data, and the cost of noncompliance.

In this issue, SearchCompliance.com Associate Editor Alexander B. Howard details the latest news on

the status of MA 201 CMR 17.00 and what business leaders, legislators and experts are saying about it.

In “[An Ounce of Prevention](#),” Richard E. Mackey outlines what data must be protected and who must comply according to the regulation as it stands today. He also offers suggestions on how to build a written information security program, or WISP, and an information security program.

Right now, MA 201 CMR 17.00 mandates encryption. In “[Encrypt It or Else ...](#)” Lisa Phifer and Rich Mogull explain technology options for encrypting laptops, portable media and wireless devices. Many organizations utilize these three types of solutions to protect confidential information or meet other regulations, such as the Sarbanes-Oxley Act.

Finally, in “[Get Ahead to Stay Ahead](#),” Linda Tucci looks at how a proactive security strategy will help business meet inevitable compliance regulations from state and federal legislatures.

We hope this e-book will help guide your companies’ decisions on how to prepare and comply with Massachusetts 201 CMR 17.00. Moreover, we hope that the security and privacy mandates included in the regulation become part of your overall security strategy, regardless of whether the Massachusetts Senate cuts back on some of the more stringent requirements. It’s the safe and secure thing to do. ■



OR COMPANY DISASTER?

An Executive Whitepaper - The Legal Risks of Customer and Employee Data Loss

Identify the **RISKS**

Understand the **LAW**

Execute the **BEST PRACTICE**

[Click Here](#) to download your free whitepaper

For more information about Becrypt
visit www.becrypt.com or call us (800) 775 0416

#becrypt

INTRODUCTION
MOVING TARGET

CHAPTER 1
IDENTITY THEFT?

CHAPTER 2
AN OUNCE OF
PREVENTION

CHAPTER 3
ENCRYPT IT
OR ELSE...

CHAPTER 4
GET AHEAD TO
STAY AHEAD

IDENTITY THEFT?

Massachusetts' tough data protection regulation still has not found its true self.

BY ALEXANDER B. HOWARD

BY NOW, MOST people have heard about, if not experienced, identity theft. Not nearly as many have heard about Massachusetts' identity theft and data protection laws and regulations.

The Massachusetts Office of Consumer Affairs and Business Regulation has received 516 data breach notifications in the past 16 months, affecting more than 800,000 residents, according to David Murray, OCABR's general counsel. Nationwide, Murray says, "10 million Americans suffer identity theft annually." And more than 94 million credit card holders were victims in the 2007 data breach of one of Massachusetts' largest businesses, The TJX Cos., in early 2007.

In response to these threats, Massachusetts enacted a security breach law (M.G.L. Chapter 93H) that went

into effect in October 2007. The law, also known as the Massachusetts Identity Theft Law, authorized the creation of specific regulations on data protection and privacy by OCABR.

The result was 201 CMR 17.00, a data protection regulation for citizens of the commonwealth that will require businesses to create and maintain a comprehensive written information security program that describes in detail where personally identifiable information (PII) resides, how it is being transmitted and what steps are being taken to protect it.

They also must implement strong user authentication protocols, encrypt records and files that contain the personal information of residents and restrict access to active users and user accounts.

Organizations also must ensure

INTRODUCTION
MOVING TARGET

CHAPTER 1
IDENTITY THEFT?

CHAPTER 2
AN OUNCE OF
PREVENTION

CHAPTER 3
ENCRYPT IT
OR ELSE...

CHAPTER 4
GET AHEAD TO
STAY AHEAD

reasonable monitoring of systems so that unauthorized use of or access to PII is detected and implement “reasonably” up-to-date firewalls and security patches to operating systems that are connected to the Internet.

Similarly, organizations must implement reasonably up-to-date versions of antivirus software that includes malware protection, patches and virus definitions. Education and training of employees on the proper use of the security systems and protocols must also be demonstrated.

In addition, the statute also requires a reasonable standard of security preparation and response to data breaches.

Despite the specificity of certain parts of the law, some of the language of how to enforce it is vague: What is a “reasonable” response to a data breach, or a “reasonable” approach to security preparation?

“I think all interpretation will be done with 20/20 hindsight based upon post-incident court outcomes,” says Seth Peter, chief technology officer at NetSPI Inc. “Many of the organizations outside of Massachusetts that I’ve spoken to do not even have this on their radar, even though they clearly fall under it with employment or credit card records. The Massachusetts organizations I’ve spoken to are aware of it but believe they are already in compliance due to existing efforts associated with GLBA, HIPAA or PCI. I do think it will undoubtedly

create a huge stir once the first significant breach is tried against it.”

Adrian Lane, senior security strategist at Securosis LLC, says he likes that “there is no loophole for companies that have a breach, had some part of their data processing or data storage encrypted, but wide open security holes elsewhere. I like the fact that they understand that mobile data is a super-set of data in motion, and that laptops and other portable devices that move data are considered at risk as well as network connections.”

The 201 CMR 17.00 regulation was originally due to begin enforcement in May, but that date has been moved to Jan. 1. (For more on what is specifically required by the regulations, see [“An Ounce of Prevention.”](#))

NOT SO FAST

Or maybe not. State officials were proud to say that 201 CMR 17.00 was the toughest such regulation in the country, but due to complaints and pushback by businesses and security experts, the Massachusetts Senate is debating Senate Bill 173 (SB 173), which seeks to amend the Identity Theft Law to take out some of the more stringent requirements, such as specific technological requirements and state jurisdiction, and whether small businesses should be made exempt.

Public hearings and debate around

INTRODUCTION
MOVING TARGET

CHAPTER 1
IDENTITY THEFT?

CHAPTER 2
AN OUNCE OF
PREVENTION

CHAPTER 3
ENCRYPT IT
OR ELSE...

CHAPTER 4
GET AHEAD TO
STAY AHEAD

SB 173 have called into doubt some of the specifics of the data protection regulation but not the intent or desire by legislatures to require businesses to safeguard PII of the residents of the commonwealth and around the country.

Peter says he sees the law as “a good start because it specifies key program elements that every company from a Fortune 100 down to a small business must consider when handling personally identifiable information.”

Mick Kless, managing partner at Regulatory Information Security Compliance (R.I.S.C.) Associates, says, “Information security officers, IT professionals and consulting firms have been telling the companies for whom they work to do this for years. But many firms, even those that are highly regulated, have traditionally taken a wait-and-see approach since they can’t seem to find the ROI. Locking down USB ports, encrypting hard drives and encrypting mail that contains sensitive data is just too ‘inconvenient’ for them. I ask them, ‘What’s your reputational risk worth?’”

Whether or not the data protection regulations are too tough depends on who is making the judgment. “Whatever protocols we put in place had to be capable of being complied with by a wide variety of businesses,” OCABR’s Murray says. “The only way to do that was to write a minimum standard where the protections

would be such that the information protected would be that which the statute said must be protected.” In his assessment, the law requires “rethinking of some standard business

“Information security officers, IT professionals and consulting firms have been telling the companies for whom they work to do this for years.”

—MIKE KLESS, MANAGING PARTNER, R.I.S.C. ASSOCIATES

principles: the basis on which we decide how much personal information we want to collect, why we want to collect it, and who gets access to it.” Murray notes that the estimated cost of a data breach is measured at \$200 for each stolen customer record. But others are not sure the statutes would necessarily represent the minimum security preparations that would be familiar to any information security professional. State Senate Chairman Michael Morrissey, who sponsored the SB 173 amendment, said in the hearing that the data protection regulation from OCABR went “beyond its intent,” as it extended jurisdiction beyond state borders and included specific technical requirements.

INTRODUCTION
MOVING TARGET

CHAPTER 1
IDENTITY THEFT?

CHAPTER 2
AN OUNCE OF
PREVENTION

CHAPTER 3
ENCRYPT IT
OR ELSE...

CHAPTER 4
GET AHEAD TO
STAY AHEAD

STATE JURISDICTION IN QUESTION

In fact, some experts say the problems with the Massachusetts regulations started in 2003, with California’s landmark data breach notification law, SB 1386.

“The groundswell started by SB 1386 has gotten a little out of control,” says Jim Hietala, research director and a principal at Compliance Research Group. “And to the extent that each new state regulation has prescriptive controls that are a little different, or have different notification requirements, it’s hard for those responsible for security and privacy at an organization to actually be in compliance. Pity the poor CIO/CISO/CPO that has to ask, ‘Let’s see, we lost a laptop with PII on it, with information on customers from all 50 states, but the data’s encrypted. Who do we have to notify?’”

ENFORCEMENT ISSUES

When it comes to enforcement, more questions surface. The OCABR is moving forward with 201 CMR 17.00 as it is currently constituted. “Our regulations were promulgated pursuant to enabling legislation that was passed in 2007,” says Barbara Anthony, recently appointed the new undersecretary for OCABR, in a statement. “This new legislative proposal differs from the enabling legislation which guided our efforts. We do not have an official comment on the new

legislation at this time except to say that it does not contain the same scope of consumer protections that our enabling legislation does.”

R.I.S.C. Associates’ Kless says he would “love to hear how the regulators plan to enforce it for those outside the banking sector, which at least makes a strong effort to comply and do the right thing.”

Kless notes that “this legislation goes hand in hand with the Red Flags identity theft prevention rule. After a deeper look, it was determined that there were more than 10 million businesses throughout the country that would need to be examined, which is nearly 10 million more than the number of examiners in the field to assess them.”

As a result, the tendency is that companies get audited only if there is an actual breach, where the holes in security would be found after the fact.

“Lack of compliance appears to be met with reasonable punishments, but will this only be enforced as breaches are reported? If so, then the laws are destined to fail before they are implemented,” says Tyler Reguly, a Toronto-based security practitioner at nCircle Network Security Inc.

Reguly says he’s “100% confident that the distinction between SMB and the enterprise is required, as is the ability for federal laws such as HIPAA to still apply. After all, you can’t expect a SMB to spend the money on securi-

INTRODUCTION
MOVING TARGET

CHAPTER 1
IDENTITY THEFT?

CHAPTER 2
AN OUNCE OF
PREVENTION

CHAPTER 3
ENCRYPT IT
OR ELSE...

CHAPTER 4
GET AHEAD TO
STAY AHEAD

ty that an enterprise is able to spend. “One of the most interesting aspects of the bill is the removal of the requirement for specific encryption technologies. The requirement still exists that the data be protected, and I’m not sure which other technologies can fill that criteria,” Reguly says. “The first time a company has a breach and isn’t using encryption it will be interesting to see how they explain it and if that explanation is accepted.”

WHAT IS TO BE DONE?

Despite the questions and doubts surrounding the regulations, no one doubts the need for data protection and privacy regulations. The guidelines just need to be more realistic, experts say, and perhaps some states will begin to look to pending federal legislation for more reasonable solutions.

“The original [Massachusetts] data protection legislation probably overreached for a state, and I understand the pushback from SMBs. Enforcement was a gap as well,” Hietala says. “I think the states tend to get into trouble when they try to get too prescriptive; the Nevada law is a good example of a poorly written law that had good intent.

“The thing I hear from customer organizations is that the proliferation of laws and regulations impacting security and privacy has created an

absolute quagmire for them, and to the extent that individual states get deeply prescriptive about the controls they need to use, it gets worse. There’s an obvious need for a federal law.” Until then, it’s still a good security practice to get in line with encryption and other safeguards, to protect now and be ready if and when federal laws appear. Securosis’ Lane says, “Heartland’s lack of end-to-end encryption was a bit of a wake-up call, especially those that rely upon third-party processors in the chain.

“We were bound to see something go beyond pure disclosure and start specifying some basic security principles without mandating specific technologies or implementation strategies. Sooner or later there will be a national version of this, or another state’s, disclosure laws,” Lane says. “We are just not there.”

Ed Moyle, a manager with Computer Task Group Inc.’s information security solutions practice and a founding partner of SecurityCurve, wrote on SearchSecurity.com that, “It’s possible that many organizations will find implementing the mandates of the law across the board to be the path of least resistance. As such, sitting up and taking notice of this law now is a pretty good idea.” (See “[Encrypt it or else](#)”) ■

Alexander B. Howard is an associate editor for SearchCompliance.com. Write to him at ahoward@techtarg.com.

“You left your laptop where?”

Strong encryption helps you comply with the Massachusetts Protection of Personal Information act



What's on your laptops, smartphones, and removable storage devices?

With the enactment of the Massachusetts Protection of Personal Information act, all companies doing business with state residents must protect any personal data both at rest and in transit. This protected information includes driver's license numbers, social security numbers, financial account numbers, or credit/debit card numbers.

With the deadline for compliance coming fast, GuardianEdge can help you implement a comprehensive plan for protecting data on your organization's end-user devices. Our enterprise-ready solutions not only safeguard data on end-points with strong encryption, but also offer the industry's lowest total cost of ownership by delivering a solution based on industry standards—enabling fast, trouble-free deployments and easy centralized management and monitoring.

To learn more, visit www.guardianedge.com

AN OUNCE OF PREVENTION

INTRODUCTION
MOVING TARGET

CHAPTER 1
IDENTITY THEFT?

CHAPTER 2
AN OUNCE OF
PREVENTION

CHAPTER 3
ENCRYPT IT
OR ELSE...

CHAPTER 4
GET AHEAD TO
STAY AHEAD

Next year, Massachusetts will enact a potentially demanding data privacy law. Here's what the law requires and what you can do today to meet the regulation.

BY RICHARD E. MACKEY

DURING ANY GIVEN week, company X discloses that it has been breached. In fact, this year alone more than 100 companies—the likes of Merrill Lynch, Pepsi and Monster.com, among others—have disclosed that personal information had been compromised.

As a result, new data protection and identity laws are taking a different approach to protecting sensitive information. While certainly not a cure-all, today's new laws are focusing on prevention rather than notification. Instead of legislating reactive data laws requiring companies to notify customers after data has been compromised, these new regulations are mandating technologies and policies in hopes of preventing a breach in the first place.

Massachusetts' 201 CMR 17.00 is

such an example. This regulation, set to go into effect in January, requires all businesses that are entrusted with personally identifiable information by Massachusetts residents to take a set of prescribed steps to protect that data.

While the law takes data privacy regulations to a new level, it also forces organizations to take some measures that are just generally good security practice. Here's what you need to know about the law and what you can do to meet the requirements and the pending deadline.

WHAT INFORMATION MUST BE PROTECTED?

The 201 CMR 17.00 regulation defines the information that needs to be protected as:

INTRODUCTION
MOVING TARGET

CHAPTER 1
IDENTITY THEFT?

CHAPTER 2
AN OUNCE OF
PREVENTION

CHAPTER 3
ENCRYPT IT
OR ELSE...

CHAPTER 4
GET AHEAD TO
STAY AHEAD

Personal information, a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

WHO IS AFFECTED?

The requirements of the law apply to persons (or organizations) that "own, license, store or maintain personal information about a resident of the commonwealth of Massachusetts." There is no concept of a "covered entity" like there is in the Health Insurance Portability and Accountability Act (HIPAA) or a clearly defined set of organizations required to comply, like there is in the Federal Trade Commission's Red Flag rules.

For those unfamiliar with those regulations, they distinguish the organizations that are directly entrusted with the sensitive information from

those that handle the data on behalf of those organizations. In the case of HIPAA, a hospital would be a covered entity, while a service provider that stored or processed the information would be considered a "business associate." In HIPAA, the law applies to only the covered entity. Covered entities are responsible for managing and policing their service providers or business associates.

Under the Massachusetts law, any organization, whether interacting directly or indirectly with Massachusetts resident information, is fully responsible to comply with the regulation.

Under the Massachusetts law, any organization, whether interacting directly or indirectly with Massachusetts resident information, is fully responsible to comply with the regulation. This difference is significant. It appears to mean that any company with personal identifying information can be prosecuted directly for a breach—rather than just the organization directly entrusted with the

INTRODUCTION MOVING TARGET

CHAPTER 1 IDENTITY THEFT?

CHAPTER 2 AN OUNCE OF PREVENTION

CHAPTER 3 ENCRYPT IT OR ELSE...

CHAPTER 4 GET AHEAD TO STAY AHEAD

information. The lack of a “covered entity” concept makes it appear as if a service provider could be legally assailed by all affected parties rather than just the company that contracted the service. There does not appear to be a way to reduce liability.

WHAT DOES COMPLIANCE MEAN?

The regulation requires organizations to safeguard personal information in both paper and electronic form against “anticipated threats” to the confidentiality or integrity of the information. What’s more, the regulation protects against the unauthorized access or use of the data that may lead to fraud or identity theft.

While the intent of the law is fairly straightforward, the regulation goes on to specify a number of requirements that some organizations, particularly small ones, might not have in place.

For example, organizations need to create and maintain a comprehensive written information security program (WISP) to secure the records containing Massachusetts residents’ personal information. Compliance with this requirement is supposed to take into account the size and resources of the business, the amount of information managed and the security requirements of the information.

The controls established need to be consistent with industry best practice and with controls specified by other

The regulation requires organizations to safeguard personal information in both paper and electronic form against ‘anticipated threats’ to the confidentiality or integrity of the information.

federal and state regulations. Further, the WISP needs to include 12 items:

- A designated person or group responsible for managing the security program.
- A method for identifying, assessing and treating risks.
- A method for improving effectiveness of security controls.
- Security policies regarding the management of personal information.
- A policy and procedure for disciplinary action in the event of policy infringement.
- A reliable method of terminating access when employees leave or are fired.
- A methodology to verify that third-party service providers will take adequate steps to secure the personal information entrusted to them.

INTRODUCTION MOVING TARGET

CHAPTER 1 IDENTITY THEFT?

CHAPTER 2 AN OUNCE OF PREVENTION

CHAPTER 3 ENCRYPT IT OR ELSE...

CHAPTER 4 GET AHEAD TO STAY AHEAD

- A practice of limiting the collection and storage of personal information to what is required.
- A practice of identifying all physical assets containing personal information to ensure they will be treated with due care.
- Regular monitoring of the security program and at least annual assessment of its effectiveness.
- Review of incidents, the organization's response activities and any corrective actions taken.
- Institution of a security education and training program for employees.

If you are acquainted with the ISO 27000 series of security standards, this list should look familiar. Virtually every one of the controls is included in those standards. Unfortunately, it is unlikely that a mid-sized or smaller company would be familiar with these standards and, more importantly, have anything resembling a written program including all these elements.

In addition to the program requirements, the regulation describes the following computer system security requirements designed to implement the policies included in the WISP:

- **Secure authentication protocols**, good identity management practices, strong passwords and automatic lockout on multiple failed logins.
- **Secure access management** that ensures that only appropriate people gain access to protected information.

- **Encryption of all personal information** that travels across public networks or on wireless networks.
- **Monitoring of systems** for unauthorized access.
- **Encryption of all personal information** stored on laptops or other portable devices.
- **Up-to-date (patched) firewall and operating systems** for all systems containing personal information connected to the Internet.

WHAT DO ORGANIZATIONS NEED TO DO?

All organizations need to step through a process to understand what they need to protect, what systems affect that information, the risks to the information and systems and the controls they should deploy to mitigate the risk. This process is described in ISO 27001, but it may seem too Draconian for many organizations to adopt. Furthermore, while developing a formal security program may be a natural part of larger organizations, smaller ones may find the process daunting.

In short form, if a company has very little in the way of a security program, it should follow this path:

1. Appoint a responsible party to lead the security program. This person should have some IT knowledge and an understanding of the information the organization has.

INTRODUCTION
MOVING TARGET

CHAPTER 1
IDENTITY THEFT?

CHAPTER 2
AN OUNCE OF
PREVENTION

CHAPTER 3
ENCRYPT IT
OR ELSE...

CHAPTER 4
GET AHEAD TO
STAY AHEAD

2. Identify the assets—in other words, identify the personal information that is in your possession and where it is. If possible, isolate it to make controlling access to the information as easy as possible.

3. Analyze the risk—consider the magnitude of risk associated with the various forms of information including where the information is stored, who has access to it, what skills an attacker would need to compromise it, the value it might have to the

attacker and the controls that might impede the attack. This practice may be beyond the reach of many non-IT organizations, so it could be a reason to seek professional help.

4. If you don't have them, **draft policies** regarding who should have access to the information and ensure that the accounts that exist on your systems and the access to paper files match that policy.

5. Establish tight controls over account creation on all your systems, disabling those for anyone who doesn't need one (or has left the company).

6. Establish a regular process of reviewing accounts and access controls.

7. Inspect your technology to ensure that you have strong passwords, good virus protection and encryption of data on portable devices and data transmitted over the Internet.

8. Ensure that employees know the importance of security of personal information to the business and their role in protecting it. You can do this by drafting a security guide or manual that describes the importance of protecting physical security of records, keeping passwords secret and following the other policies you have defined. Reinforce this documentation with regular training.

TECHNOLOGY REQUIREMENTS

MUST-HAVE TECHNOLOGIES:

- ▶ Laptop encryption
- ▶ Portable device encryption
- ▶ Firewalls
- ▶ Antivirus software
- ▶ Patch management software
- ▶ Authentication system that supports lockout after multiple failures.

NOT REQUIRED, BUT USEFUL:

- ▶ Monitoring software to help analyze logs and system use.
- ▶ Intrusion detection systems
- ▶ Identity management software
- ▶ Vulnerability management

INTRODUCTION
MOVING TARGET

CHAPTER 1
IDENTITY THEFT?

CHAPTER 2
AN OUNCE OF
PREVENTION

CHAPTER 3
ENCRYPT IT
OR ELSE...

CHAPTER 4
GET AHEAD TO
STAY AHEAD

9. Draft a procedure for responding to incidents like information leakage, virus infections and any other security compromise. This could mean calling in IT support personnel to help sort out the problem, but it's critical to outline the steps leading to bringing in outside help.

10. Make sure systems are configured to lock out users after multiple failed login attempts

11. Establish a process for monitoring who logged in to systems storing personal data with specific provisions for identifying unauthorized access.

12. Ensure that all systems with personal data on them are protected by a firewall and are running up-to-date software.

13. Identify all external parties with whom you share personal information. Their treatment of the data is critical to your compliance. Ask each of them for some evidence that they comply with the requirements of the law. If possible, avoid exposing the data to them to bypass the problem altogether.


These steps describe activities that all companies should follow to ensure that their sensitive data is protected. Unfortunately, some organizations may not have the IT staff and the security skill to take these tasks on,

but this should not be a reason to ignore the problem. The most important step is to take the time to think about your data and to know where it is stored and who has access to it. The better contained the information is, the easier the IT problems become. The rest of the steps can be done with the help of IT contractors.

Larger organizations face a different problem. While they may have the IT staff, many will not have the formal, documented security policies and procedures that would meet the requirement of a WISP. Further, they may not have established the kinds of organizational roles, service provider management processes, monitoring and incident response procedures for which the regulation calls. These companies simply have to bite the bullet and do what it takes to comply.

If you take a more global view, the steps you take to address these requirements should improve your overall security approach. After all, it pays to recognize that this law is likely the first of a long line of state and federal laws that will require the same types of controls. ■

Richard E. Mackey, vice president, SystemExperts Corp., ISACA/CISM, is a leading authority on enterprise security architecture and compliance. Before joining SystemExperts, Mackey was director of collaborative development for The Open Group (the merger of the Open Software Foundation and X/Open). Prior to the merger, he was technical lead of the OSF Distributed Computing Environment project.



**Devices come and go,
but your data should never leave.**

**Application for FIPS
140-2 Certification
In Progress**

**Reduce Your
Insider Risk**

**Enforce Removable
Media Policy**

Proactive Malware Protection



Learn how to effectively protect your vital information by going to our resource center at

www.lumension.com/security-tip-60

1.888.725.7828

DATA PROTECTION: The cost of mobility is high.

Unmanaged removable devices, like USB sticks and PDA's, put your data at risk through data leakage and malware introduction. Lumension® Data Protection gives you the power to enable the secure use of these devices – letting you run your business effectively while protecting your data on the go.

Vulnerability Management | Endpoint Protection | Data Protection | Reporting and Compliance

ENCRYPT IT OR ELSE...

INTRODUCTION
MOVING TARGET

Like PCI, MA 201 CMR 17.00 is mandating encryption. Here are some approaches you can take.

BY LISA PHIFER AND RICH MOGULL



CHAPTER 1
IDENTITY THEFT?

CHAPTER 2
AN OUNCE OF
PREVENTION

CHAPTER 3
ENCRYPT IT
OR ELSE...

CHAPTER 4
GET AHEAD TO
STAY AHEAD

IN ITS CURRENT form, the new Massachusetts data privacy law, 201 CMR 17.00, mandates data protection by way of encryption. Specifically, the law states that any firm conducting business with state residents needs to protect personally identifiable information, which includes a person's name along with his Social Security number, bank account number or credit card number, and the information must be encrypted when stored on portable devices or transmitted wirelessly on public networks.

Encryption of personal information on portable devices such as laptops, personal digital assistants (PDAs) and flash drives must also be completed by Jan. 1, according to the Massachusetts Office of Consumer Affairs and Business Regulation.

We'll explain the options you can put in place to meet the regulation.

LAPTOP ENCRYPTION OPTIONS

File and folder encryption: To meet these demands, most businesses will choose IT-administered stored data protection, based on file/folder encryption, full-disk encryption or some combination thereof. File/folder encryption is also selective but encrypts files automatically, based on defined attributes like file location (e.g., folder), file type (e.g., spreadsheets) or source application (e.g., everything Excel touches).

For example, the Windows Encrypting File System (EFS) is Microsoft's basic file/folder encryption tool. It can be centrally activated by using Active Directory Group Policy Objects (GPOs) to encrypt specified files or folders. However, EFS still relies on sensitive data being written into protected locations and cannot stop users from copying encrypted

INTRODUCTION
MOVING TARGET

CHAPTER 1
IDENTITY THEFT?

CHAPTER 2
AN OUNCE OF
PREVENTION

CHAPTER 3
ENCRYPT IT
OR ELSE...

CHAPTER 4
GET AHEAD TO
STAY AHEAD

files to unencrypted locations (e.g., thumb drives).

More sophisticated file/folder encryption products do more. For example, some offer stronger policies that make data leakage less likely, provide reports that document compliance after a laptop goes missing and can apply a consistent encryption platform and policy to heterogeneous devices, e.g., PCs, PDAs and removable storage.

Full-disk encryption: For general-purpose computers, the other popular approach is to simply encrypt everything stored on a physical disk or a logical volume. The goal is to ensure that nothing is ever written to storage without being encrypted. That includes not only sensitive user data, but also application and operating system files.

An example of volume encryption is the BitLocker feature in Windows Vista. It divides a PC's boot drive into an unencrypted boot volume and an encrypted operating system volume, which is unlocked and verified at boot time using a Trusted Platform Module chip, USB key or recovery passphrase. But data written to non-OS volumes is still unprotected, although it can optionally be encrypted using EFS.

More comprehensive full-disk encryption (FDE) scrambles the entire hard drive's contents, including boot sectors, swap files, OS files and user data. Authentication, encryption,

provisioning and reporting capabilities vary, but enterprise FDE products offer features like Windows single sign-on and central logging for security audit and compliance reporting.

Comparing alternatives: The main weakness of file/folder encryption is the possibility of data leakage. So why doesn't everyone use full-disk encryption? For starters, encrypting an entire disk can take hours—not including the time required to make a full system backup first. Thereafter, all data will be encrypted "on the fly," slowing overall system performance to some (not necessarily noticeable) degree.

Some FDE pre-boot authentication methods interfere with other programs that may also be used on the protected system, from asset-tracking products to sign-on processes that modify the Windows graphical identification and authentication library. Moreover, desktop administration, patching and auditing tools and practices may be affected, since they cannot unlock encrypted system files without the user's credentials. If a protected system is corrupted or damaged, data recovery can be similarly affected. Finally, when routine backups are created, it's wise to encrypt those, too.

Combining methods can enable an organization to obtain the best of both worlds. For example, use file/folder encryption on less capable devices like PDAs, while applying FDE

INTRODUCTION MOVING TARGET

CHAPTER 1 IDENTITY THEFT?

CHAPTER 2 AN OUNCE OF PREVENTION

CHAPTER 3 ENCRYPT IT OR ELSE...

CHAPTER 4 GET AHEAD TO STAY AHEAD

to laptops. Applying both methods to the same device might seem like overkill, but it is a viable option—particularly for mobile users who carry regulated data. FDE offers foolproof protection against device loss or theft, while file/folder encryption can protect sensitive user data without obscuring files that IT requires to perform maintenance and recovery tasks.

Of course, the decision will also be influenced by workforce size and budget, privacy needs, risk tolerance and company politics.

PORTABLE MEDIA PROTECTION

While it's fairly straightforward to protect a laptop using full-disk encryption, portable media presents more challenges. Mobile employees often have a legitimate need to use such devices to transfer data, even sensitive data, while on the road. At one time specialized hardware was considered for this task, but prices have dropped so much that even gigabyte thumb drives are routinely handed out for free on conference floors, and it's hard to find a laptop without a CD or DVD burner included as standard.

Although there are still a few organizations sending techs out armed with hot glue guns to gum up the USB ports and read-only CD drives on their client machines, most enterprises rely on a slew of software options to manage these potential

leak points. Let's review a few of them below:

1. On Windows XP and Vista, group policy objects can be used to restrict device installation. Vista offers more granular policies than XP, but devices already installed by the user may still be accessible depending on how the GPO is configured. This option is free, but it is not as flexible as alternatives, and it may not offer as much security.

2. A variety of third-party software tools can restrict access to portable storage, including CD-ROM and USB devices. Policies can be extremely granular, allowing access to only corporate-approved devices, or allowing read-only connections to digital cameras and music layers while still preventing outbound data transfers. Most tools support role- and system-based policies, allowing restrictions for different user and computer groups (e.g., completely disabling write access for desktops, while allowing it for executive laptops).

3. Third-party software can block or audit access to portable storage. Policies can allow access while keeping a secure copy of the files, which are then sent to the management server the next time the laptop connects to the corporate network. An administrator can then review the

INTRODUCTION MOVING TARGET

CHAPTER 1 IDENTITY THEFT?

CHAPTER 2 AN OUNCE OF PREVENTION

CHAPTER 3 ENCRYPT IT OR ELSE...

CHAPTER 4 GET AHEAD TO STAY AHEAD

activity, including the contents of the file, to see if it complies with policy.

4. Encryption software can be used for optional or mandatory encryption of data on portable storage. Users can choose (depending on policy) between corporate and group keys, or self-decrypting archives with password protection for transfer to partners not using the same encryption software. Some tools can apply policies based on user, group, system or even storage device.

5. Dedicated USB devices can be tied to central policies. This is probably the most expensive option, and such devices don't offer material security benefits over software solutions.

6. Data loss prevention (DLP) products with endpoint protection can be used. These tools can apply dynamic policies based on detected content. For example, a file with credit card numbers can be restricted, while a PowerPoint presentation with no sensitive content can be transferred. The best tools use deep content analysis to protect not only easily recognizable data like credit card and account numbers, but also less structured data like portions of protected documents. Some tools include or partner for encryption. DLP is the most flexible option, and all tools will eventually have to include content-

based capabilities. They are more complex to define policies for, however, and maturity levels vary greatly.

Enterprises have a wide variety of options, from simply blocking devices to real-time content-based policies tied to dynamic encryption. The best option for your organization will depend on your specific needs, user tolerance, budget and existing infrastructure.

WIRELESS ENCRYPTION

Wi-Fi Protected Access (WPA) has been standard technology on all wireless equipment. WPA and WPA2-Enterprise provide robust WLAN access control, but deploying 802.1X can be overwhelming for companies with limited IT staff and budget

Outsource 802.1X services: WPA and WPA2-Enterprise use the 802.1X port access control framework to authenticate wireless users. This framework pairs with authentication servers commonly found in corporate networks, like RADIUS servers, Windows Active Directories, RSA SecurID Authentication Managers and Certificate Authorities. Companies that do not have an authentication server and prefer not to install one can outsource this component to a third party like BoxedWireless or WiFiRadis.

These providers offer managed Wi-Fi authentication services. Instead

INTRODUCTION MOVING TARGET

CHAPTER 1 IDENTITY THEFT?

CHAPTER 2 AN OUNCE OF PREVENTION

CHAPTER 3 ENCRYPT IT OR ELSE...

CHAPTER 4 GET AHEAD TO STAY AHEAD

of consulting your own local RADIUS server, your access points (APs) forward 802.1X / Protected Extensible Authentication Protocol (PEAP) messages through a Transport Layer Security (TLS) tunnel, across the Internet, to the provider's RADIUS server. That server validates the station's identity and password before granting or denying access to your WLAN. Usernames can be added to and removed from your account through an administrator Web portal.

These services differ in detail—for example, BoxedWireless supports both EAP-TLS and PEAP/MSCHAP v2, while WiFiRadis supports only the latter. BoxedWireless is a commercial service, while WiFiRadis is free. Either way, basic setup is easy. By outsourcing 802.1X services, you can achieve “enterprise” security with little more effort than it takes to configure “personal” pre-shared secrets. However, bear in mind that these services are intended to fill a gap for very small businesses; they are not business-oriented managed security products.

Roll your own 802.1X infrastructure:

Some companies would rather have their own authentication server but lack the budget to buy a commercial RADIUS product. Another option is freely available RADIUS server software like FreeRADIUS. But don't kid yourself: Rolling your own RADIUS server will require spare hardware, tech savvy and at least a little sweat.

To run FreeRADIUS, you'll need spare time and server hardware running Linux, FreeBSD, OpenBSD, OSF/Unix or Solaris. FreeRADIUS is released under the GNU General Public License, which means it is free to download and install. When used as a wireless authentication server, FreeRADIUS can process EAP-MD5, EAP-SIM, EAP-TLS, EAP-TTLS, EAP-PEAP and LEAP access requests. Security policies, server configurations and user credentials are all up to you. But once you've invested the effort, you'll have a flexible RADIUS server that can be used for other purposes, like remote user virtual private network authentication. Advice on configuring FreeRADIUS for wireless can be found at http://wiki.freeradius.org/WPA_HOWTO.

Alternatively, consider turning a Microsoft Windows Server into a RADIUS server for your WLAN. If you have a spare PC running Windows Server 2003, it can be configured to run Microsoft's Internet Authentication Server (IAS). To learn how to set up IAS for use with 802.1X, visit <http://technet.microsoft.com/en-us/network/bb643123.aspx>. If you have a spare PC running Windows Server 2008, you can accomplish similar results using Microsoft's new Network Policy Server. While these solutions are not open source, they can help you roll your own RADIUS server using products and platforms that you already own.

INTRODUCTION MOVING TARGET

CHAPTER 1 IDENTITY THEFT?

CHAPTER 2 AN OUNCE OF PREVENTION

CHAPTER 3 ENCRYPT IT OR ELSE...

CHAPTER 4 GET AHEAD TO STAY AHEAD

Skip 802.1X altogether: Companies that find the whole idea of 802.1X overwhelming can use WPA or WPA2-Personal instead. These “personal” measures still represent an improvement over Wired Equivalent Privacy when based on a strong pre-shared key (PSK).

When PSKs are too short or composed of words found in the dictionary, they can easily be guessed. An attacker simply needs to capture a few packets exchanged by a legitimate user when connecting to the WLAN, then run a dictionary attack tool like coWPAtty. To prevent this, choose a PSK value that’s at least 20 random alphanumeric characters. For best results, use a random password generator and include numbers and mixed case (e.g., T2adREfasACach64a6Us). Better yet, if your AP and client support Wi-Fi Protected Setup (WPS), configure a long, random PSK by pushing the button on the front of your AP or by typing a client-generated WPS PIN into your AP’s GUI.

Furthermore, when using PSKs, it’s important to assign your WLAN a relatively unusual network name (extended service set identifier, or ESSID). Why? PSKs can be guessed much faster by contemporary cracking tools when your WLAN uses a common default ESSID. Here again, WPS can be used to configure a “good” ESSID for you.

No matter how random or long your PSK might be, users connected

to your WLAN must know that value or have it configured into their systems. A configured password makes life easier because users don’t have to remember or correctly type a long, random string. But that configured password will be compromised if someone loses a laptop or leaves it unattended. On the other hand, prompting for PSKs increases the chance that users will give them to guests, write them down on sticky notes or otherwise disclose the entire WLAN’s password.

Updating your WLAN’s PSK at regular intervals can help reduce risk but, ultimately, group passwords can only take you so far. If your company is really concerned about keeping outsiders off your WLAN—or knowing who is using your WLAN at any point in time—then upgrade to WPA or WPA2-Enterprise. ■

EDITORS’ NOTE: This information was originally published on SearchSecurity.com. While 201 CMR 17.00 is mandating encryption for laptops, USB devices and information transmitted over wireless networks, a new Senate bill, SB 173, proposes to make revisions to these specific requirements. At press time no resolution has occurred.

Lisa Phifer is president of Core Competence Inc. **Rich Mogull** is the founder of Securosis LLC, an independent security consulting practice.



January 2010 is fast approaching. Are you ready?

If you're conducting business with customers within the Commonwealth of Massachusetts, you're running out of time before their sweeping data protection law goes into effect.

Razorpoint's Network Security Umbrella includes everything you need to develop, implement, maintain and monitor a security system compliant with 201 CMR 17.00, including:

- ✓ Control of user IDs
- ✓ Secure method of assigning and selecting passwords
- ✓ Secure method of protecting passwords
- ✓ Restrict access to active users only
- ✓ Blocking access to user ID after multiple unsuccessful attempts
- ✓ Restrict access to records and files only to those who need it
- ✓ Assign unique ID & passwords
- ✓ Encrypt all records containing personal information transmitted across public networks
- ✓ Monitoring of systems for unauthorized use
- ✓ Encrypt all data containing personal information to be transmitted wirelessly
- ✓ Encryption of all personal information stored on laptops or other portable devices
- ✓ Implement firewall protection for personal information on a system connected to the Internet
- ✓ Apply OS security patches for files containing personal information on systems connected to the Internet
- ✓ Deploy malware protection
- ✓ Deploy virus protection
- ✓ Apply up-to-date patches on security agent software
- ✓ Develop a written information security program (WISP) to protect personal information
- ✓ Establish a means for detecting and preventing security system failure
- ✓ Secure storage and back-up of data
- ✓ Annual review of security measures
- ✓ Ensure that third party service providers deploy security measures consistent with 201 CMR 17.00
- ✓ Train employees on proper use of computer security practices

For more information on how to get your company compliant before January 2010, call a Razorpoint representative at 212.744.6900 ext. 103, email secure.now@razorpoint.com, or visit www.razorpoint.com.



GET AHEAD TO STAY AHEAD

Despite appearances, the Massachusetts data protection law does offer opportunities for those who act proactively.

BY LINDA TUCCI



ASK INTERNET entrepreneur-turned-retailer Dennis Kelly how he feels about the new Massachusetts personal data protection standards that are scheduled to take effect next year, and you'd think the great commonwealth of Massachusetts had fashioned them as a marketing tool just for him.

"Given what has happened with various retailers, systems getting hacked, we figured we needed to get out ahead of it as aggressively as possible and use it as an opportunity to create a higher level of trust with our customers," Kelly says.

Kelly co-owns Wireless City, a fast-growing chain of 27 wireless stores that can be found in Florida, Georgia and Massachusetts. In business five years, the chain is an exclusive licensee for Verizon wireless products and its motto is that buying a cell phone

should be fun, not painful. Or lead to identity theft.

To purchase wireless devices, customers need to give carriers their Social Security numbers. "People are hesitant and concerned when they give that number out along with a whole bunch of other personal information," he says.

Adhering to 201 CMR 17.00, as the regulation is called, makes good business sense, he says. Indeed, Kelly has spent close to \$10,000 on professional services from security expert Kurt Baumgarten, CISA and vice president of information security at Peritus Security Partners LLC, to ensure his enterprise fulfills the 201 CMR 17.00 compliance checklist and more. When all the boxes are checked, he says he plans to install signs advertising that fact at every cash register in his stores.

INTRODUCTION
MOVING TARGET

CHAPTER 1
IDENTITY THEFT?

CHAPTER 2
AN OUNCE OF
PREVENTION

CHAPTER 3
ENCRYPT IT
OR ELSE...

CHAPTER 4
GET AHEAD TO
STAY AHEAD

INTRODUCTION MOVING TARGET

CHAPTER 1 IDENTITY THEFT?

CHAPTER 2 AN OUNCE OF PREVENTION

CHAPTER 3 ENCRYPT IT OR ELSE...

CHAPTER 4 GET AHEAD TO STAY AHEAD

AS MASSACHUSETTS GOES, SO GOES THE NATION

Wireless City's take on the regulation is something of an exception, judging from the complaints registered by many of the 64 companies that filed letters during the public comment period, including Verizon in a Jan. 15

There is also a movement to look “more upstream and take a more holistic view of data protection.”

—IAN GLAZER
ANALYST, BURTON GROUP INC.

letter. And the comprehensive standards may be subject to change. There is legislation introduced in the Massachusetts Senate that would water down the requirements.

Still, Wireless City is probably smart in getting ahead on the security requirements. Many analysts believe the commonwealth's decision to make firms take a proactive, policy- and procedure-based approach to data protection is the wave of the future, likening 201 CMR 17.00 to California's groundbreaking data breach notification law passed in 2003. After that law was passed and strengthened, 44 other states not only followed suit but also have been ramping up their post-breach penalties.

There is also a movement afoot on the federal level to look “more upstream and take a more holistic view of data protection,” says analyst Ian Glazer of Burton Group Inc. H.R. 2221, a federal bill moving through committee on the Hill, “talks a lot more about data protection than post-breach penalties,” Glazer says, adding that he would not be surprised to see some kind of federal legislation on data protection by year's end.

WHAT WILL IT COST: THE STATE'S NUMBERS

Type *Mass. data privacy law* into Google and a list of advertisements pops up in the right-hand margin. There are kits you can purchase, security experts for hire, consultants, law firms at the ready. So what will it cost companies to comply? According to the state's Fiscal Effect and Small Business Impact Statement, a hypothetical small business with 10 employees should pay no more than \$3,000 a year.

The analysis, which is worth reading in full, assumes the hypothetical company has three laptops and one network server serving seven desktops, as well as multiple, lockable file cabinets—oh, yes, and an expert on hand: “...we think it more than likely that a 10-employee business would already have retained such a consultant to monitor and maintain the current installation and software in con-

INTRODUCTION
MOVING TARGET

CHAPTER 1
IDENTITY THEFT?

CHAPTER 2
AN OUNCE OF
PREVENTION

CHAPTER 3
ENCRYPT IT
OR ELSE...

CHAPTER 4
GET AHEAD TO
STAY AHEAD

nection with protecting the company's own, and customer, information." If the business does not have an existing technical support program, make that \$6,000, or \$500 per month in consulting fees (see sidebar).

IT'S THE DATA, NOT THE COMPUTERS
Before rushing to spend \$3,000 or \$6,000 or more on complying with 201 CMR 17.00, it is important to understand what the regulation does and does not require.

**\$3,000 OR LESS TO COMPLY
WITH 201 CMR 17.00?**

IN ITS FISCAL Effect and Small Business Impact Statement, the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) estimates that small and medium-sized businesses (SMBs) with 10 employees, for example, should pay no more than \$3,000 to comply with the consumer data protection requirements laid out in 201 CMR 17.00. CIO Gerry Young says he believes the cost of compliance could be even less.

"What we've been doing is working with the SMB to find as much freeware, shareware, open source code as we can. I think we can actually drive some of that cost down," says Young, who was until recently CIO of the OCABR and is now Secretariat CIO of the Executive Office of Housing and Economic Development.

He argues that businesses or consulting firms that claim the costs of compliance will in fact be much higher than \$3,000 have an antipathy toward using open source and free software. "Yet if you look at the state of freeware, shareware, open source code you can't dismiss out of hand what they can do to contribute to this [data protection] model. Free options are out there to encrypt USB drives, laptops and PCs, requiring only the labor cost to do it."

Much of the technology needed to comply comes with the equipment many companies already own.

Indeed, he says he does not believe the rough spots for complying with 201 CMR 17.00 will be technology-related. But if there is an issue, it is the regulation's push to make key management front and center. "That, I think, will be the biggest issue for SMBs," Young says, because "they are just not used to dealing with symmetric and asymmetric keys and being able to hang on to the keys to decrypt."

Asked if that would not require hiring an expert, Young notes that key management-for-dummies-type books might cost \$20. "Even if people don't understand all of the technical details behind key management, it is not going to take much education to bring them up to speed." —L.T.

INTRODUCTION
MOVING TARGET

CHAPTER 1
IDENTITY THEFT?

CHAPTER 2
AN OUNCE OF
PREVENTION

CHAPTER 3
ENCRYPT IT
OR ELSE...

CHAPTER 4
GET AHEAD TO
STAY AHEAD

Technology consultant Sarah Cortes says the first mistake companies make is to think the law is about computer hardware.

"The law does not apply to laptops, computers or machines; it applies to data," says Cortes, a principal at Cambridge, Mass.-based Inman TechnologyIT. "The law is not saying you have to get your laptop encrypted; it is saying you have to encrypt your data if it meets certain criteria."

Therein probably lies one of the most difficult tasks required of the law. Many companies, small, medium or large, don't know what data they have, or may know less about their data than they think they do. Data inventory is a big job, even more so when it involves archived data. "Even world-class companies don't really know what they have; they realize they have vast amounts of data in files all over the place," says Cortes, who counts Fidelity among her clients.

In addition, many companies believe that if they do collect confidential data they must encrypt it and meet the 20 requirements of the regulation. But the personal data protected by the law must contain a name and another piece of personal identifying information, such as a Social Security number or bank account number.

"It's like a combination lock," Cortes says. "There will be a lot of companies that have the requisite combination,

but there will be many that don't, and they need to know, 'Oh, you're done. Don't worry about anything else.'"

WHAT'S A SMALL COMPANY TO DO?

Large companies have many resources at hand to sort out the data, as well as automated tools used to meet other compliance mandates, such as the Sarbanes-Oxley or Health Insurance Portability and Accountability acts. What about the small, privately owned company never or rarely subject to compliance regulations before—for example, a clothing boutique or independently owned dry cleaners?

The first question small business owners need to ask, Cortes says, is whether they are keeping personal records such as payroll or credit card data on their computers. It may be that the company uses an accountant to process paychecks, in which case the data is the accountant's problem to protect because he or she is the one storing it, Cortes says. With regard to credit card data, the question is whether the business is storing it or using a facility that passes that information off-site to a company like PayPal, which stores the information. A really small company might not have any of this data stored and it is done, Cortes says.

Or it might be storing the Social Security numbers of 10 employees and indeed fall within the purview of

INTRODUCTION
MOVING TARGET

CHAPTER 1
IDENTITY THEFT?

CHAPTER 2
AN OUNCE OF
PREVENTION

CHAPTER 3
ENCRYPT IT
OR ELSE...

CHAPTER 4
GET AHEAD TO
STAY AHEAD

the law.

Before that small business rushes to beef up security, Cortes advises that it think hard about alternatives to storing the data. “Everybody jumps to the conclusion that they have to figure out how to get compliant, instead of asking why they are storing the data,” she says.

Many companies
don’t know what
data they have.

Cortes cites a recent client, a Web design firm in New York that’s the creative talent behind some very high-profile websites, including the one for the Guggenheim Museum. The midsize design firm, which boasts about 300 clients, had suffered a data breach. A hacker stole some information from a plastic surgeon who sold products online—the only client this design firm had put on its own server. “I advised her to think through what it would cost to make that one site compliant. I said, ‘It’s not your core business, it is on a platform you built three years ago that probably should be updated anyway, and you’re taking on this liability,’” Cortes recalls. She advised the firm to get the personal data off its site.

“A lot of companies are not big enough to deal with the risk of credit cards, or with Social Security num-

bers,” Cortes says, “You can change your workflow and not accept the risk.”

THE HOLISTIC APPROACH

Peritus’ Baumgarten, the consultant for Wireless City, agrees that many businesses will be thrown for a loop by the new reg. “This is going to hit a lot of people with this who never had to comply with anything,” he says, adding he believes many of the smallest companies will decide they just don’t have the time or money to comply.

In his view, it is the broad middle swath of businesses—not large enough for sophisticated data protection policies and procedures but with a lot to lose if they run afoul of the law, that are most affected.

“They certainly don’t want to be held up as the poster child for non-compliance,” he says. “And they will, as we are seeing now, generally do their best to at least get the ball rolling.”

Baumgarten recommends those companies that fall in this group first do a security assessment to identify their risks because the next step—creating the written information security program (WISP)—is a big project.

His firm has a 36-page risk self-assessment application that is online and breaks down the regulations “in layman’s terms.” Customers can fill that out to define where their risk lies in regard to information security and

INTRODUCTION MOVING TARGET

CHAPTER 1 IDENTITY THEFT?

CHAPTER 2 AN OUNCE OF PREVENTION

CHAPTER 3 ENCRYPT IT OR ELSE...

CHAPTER 4 GET AHEAD TO STAY AHEAD

what will be expected of them by the state. The exercise also includes videos of Baumgarten and his colleagues explaining various aspects of the law, which helps fulfill the education and training components of the law.

The self-assessment then serves as the basis for a professional risk assessment, cutting down on the time and expense of having the firm do the preliminary work. The entry price for the risk assessment is \$795, which includes some consulting time. The next step would be writing a WISP—prices vary by the size and complexity of the company.

As for how precisely to comply with the law, Baumgarten's firm works off the ISO 27001 standards, which were also used to develop 201 CMR 17.00. Rather than inventory the data, "We often say why not throw a big warm fuzzy blanket over everything and treat it all the same? Think about the administrative nightmare you're mitigating by not cherry-picking every piece of data that might be categorized as critical Massachusetts resident data and trying to treat it differently than everything else," says Baumgarten, whose firm is vendor-agnostic and does not sell technology tools.

"If you have to implement the controls anyway, how about protecting all the information in your organization?" he says. "This is a new world out there. Everything is critical." ■

Linda Tucci is a senior news writer for SearchCompliance.com. Write to her at ltucci@techtarget.com.



*The Massachusetts Data Protection Law:
What It Is and How to Deal With It*
is produced by CIO/IT Strategy Media
and Security Media,
© 2009 by TechTarget

MANAGING EDITOR, CIO/IT STRATEGY MEDIA GROUP
Jacqueline Biscobing

ART DIRECTOR
Linda Koury

CONTRIBUTING WRITERS
Alexander B. Howard,
Richard E. Mackey,
Lisa Phifer,
Rich Mogull and
Linda Tucci

EDITORIAL DIRECTOR, SECURITY MEDIA GROUP
Kelley Damore

EXECUTIVE EDITOR, CIO/IT STRATEGY MEDIA GROUP
Scot Petersen

FOR SALES INQUIRIES:
Stephanie Corby,
Senior Director of Product Management,
scorby@techtarget.com
(781) 657-1589

BUSINESS STAFF
SENIOR VICE PRESIDENT AND GROUP PUBLISHER
Andrew Briney

PUBLISHER, SALES
Jillian Coffin



Focused on finance?

Introducing SearchFinancialSecurity.com!

Now there's an online resource tailored specifically to the distinct challenges faced by security pros in the financial sector. *Information Security* magazine's sister site is the Web's most targeted information resource to feature FREE access to unbiased product reviews, webcasts, white papers, breaking industry news updated daily, targeted search engine powered by Google, and so much more.

Activate your FREE membership today and benefit from security-specific financial expertise focused on:

- Regulations and compliance
- Management strategies
- Business process security
- Security-financial technologies
- And more

www.SearchFinancialSecurity.com



SearchFinancialSecurity.com

The Web's best information resource for security pros in the financial sector.

TechTarget
Security Media



INFORMATION
SECURITY

INFORMATION SECURITY DECISIONS



#becrypt

- ▶ [The Legal Risks of Data Loss—Free white paper](#)

GuardianEdge

- ▶ [Data Privacy eSeminar: Complying with New State Data Privacy Legislation](#)
- ▶ [Weekly Product Demo: Eliminating Data Loss and Leakage in the Enterprise](#)
- ▶ [White Paper: Protecting Enterprise Data on the Endpoint](#)



- ▶ [Protecting Your Vital Information Resource Center](#)
- ▶ [Discover Every Device on Your Network](#)
- ▶ [New Insider Threat Emerges in the New Economy](#)



- ▶ [Learn How To Become Compliant with MA 201 CMR 17.00](#)
- ▶ [Assess the Security of Your Network](#)
- ▶ [Rz.EndPoint Protects the Security of your Laptops and Desktops](#)

SOPHOS

- ▶ [Upcoming Sophos Web Seminars](#)
- ▶ [Safeguard Enterprise: Your Central Key for Enterprise Protection](#)
- ▶ [White Paper: The Business Impact of Data Security Regulations: Featuring Massachusetts.](#)