WKH PDVVDFKXVHWWV GDWD SULYDFB ODZ - ZKDW EXVLQHVVHV QHHG WR NQRZ DQG GR

Presented by:

Brad Dinerman
Fieldbrook Solutions LLC

November 17, 2009

Encryption Primer

To get from:

WKH PDVVDFKXVHWWV GDWD SULYDFB ODZ - ZKDW EXVLQHVVHV QHHG WR NQRZ DQG GR

You need a key, such as:

Real Letter = Letter You See - 3

So you get:

THE MASSACHUSETTS DATA PRIVACY LAW - WHAT BUSINESSES NEED TO KNOW AND DO

fieldbrook solutions LLC

MGL 201 CMR 17.00

Standards for the Protection of Personal Information of Residents of the Commonwealth.

Sometimes referred to as “The Encryption Law,” but encryption is really only one small part of it.

Preliminary

Thank you to Michael Castro
of *Castro, Thresher & Oliveira*
for the opportunity to speak with you.

fieldbrook solutions LLC

Objectives of This Presentation

1. Discuss the new data privacy law (not just the “encryption law”).
2. Identify key points of the law and create a “road map” for your business.

fieldbrook solutions LLC

Who Am I?

Founder and president of Fieldbrook Solutions LLC
Provide IT and MIS consulting services in eastern MA

- Microsoft MVP (Enterprise Security)
- Microsoft Certified Systems Engineer (MCSE)
- Certified Information Systems Security Professional (CISSP)
- Certified SonicWall Security Administrator (CSSA)
- Founder and President, National Information Security Group (NAISG)
- Member of FBI Infragard

fieldbrook solutions LLC

MGL 201 CMR 17.00

What is it?

- A new law to protect the privacy (and therefore, identity) of residents of Massachusetts
- A law which WILL affect YOU and the way you do business.

When does it take effect?

- March 1, 2010

When should my business start preparing?

- Last month

fieldbrook solutions LLC

Personal Information Is Everywhere

Personal Information (PII) =

First name/initial + last name + any of the following:

- Account number, credit or debit card number
- Social Security number;
- Driver's license number or state-issued ID;
- Passport ID

Personal Information Is Everywhere

Sources of Personal Information in your files may include:

- Employee Applications
- I-9 Forms
- Tax Forms (Federal W4 and State)
- Payroll/Direct Deposit Forms
- Benefit Applications
- Medical or Disability Forms
- Retirement Plan Forms
- Employee Stock/Option Plans
- Visa & Immigration Records
- Payroll Reports
- Employment Agreements
- Contractor Agreements
- Bonus/Incentive Plans
- Timesheets
- Compensation Reviews
- Census Data
- Background Checks
- Credit Checks

fieldbrook solutions LLC

Risks Of Loss Are Widespread And Costly

Widespread risks via technology

- 90% of data loss occurs electronically
- Risks increases exponentially once data leaves database or application

Risk of Information Loss

High Risk	USB devices/Disks BlackBerry/ Portable Phones Instant Messaging Email
Medium Risk	Laptops & Home PCs Corporate Workstations File Servers
Low Risk	Centralized Applications Databases

fieldbrook solutions LLC

Risks Of Loss Are Widespread And Costly

Employees are typically the weak link

- 40% of MA breaches due to “employee sloppiness”
- 60% of employees take data when leaving job

MA law increases stakes

- Escalates industry standards (PCI, GLB, HIPAA) to law
- Prosecution by Attorney General and/or class action suits
- Costs of breach estimated at ~$200/record
- Legal and PR costs per incident start in tens of thousands of dollars

fieldbrook solutions LLC

The Compliance Roadmap

Don’t wait until February 28.

Put your plans into place now,

and avoid this:

fieldbrook solutions LLC

Mile 1 – Write the WISP

Written Information Security Plan (WISP) should include:

- Description of administrative, technical, and physical safeguards for PII protection
- Name of employee who will maintain and supervise WISP implementation and performance (Data Security Coordinator)
- Identification of the paper, electronic and other records, computing systems, and storage media, including laptops and portable devices, that contain personal information
- Description of regular, ongoing employee training, and procedures for monitoring employee compliance
- Disciplinary measures for violators
- Policies and procedures for when and how records containing PII should be allowed to kept, accessed or transported off your business premises

Mile 1 – More WISP Items

- How you block terminated employees' physical and electronic access to PII records
- That you've verified that any third-party service provider with access to PII has the capacity to protect such personal information in the manner provided for in 201 CMR 17.00
- That you've identified that the length of time that you are storing records containing PII is limited to the time reasonably necessary to accomplish your legitimate business purposes and/or to comply with state or federal regulations
- That access to your PII records are limited only to those who have a need to know
- How you restrict physical access to PII
- How you regularly monitor/audit access to PII
- How often you review polices and procedures and update the WISP
- How you will handle any "incidents"

Mile 2 – The Data Security Coordinator

Appoint a Data Security Coordinator ("Volunteers, anyone?")

This individual will be responsible for overseeing your organization's compliance with the law.

He/she does not need to be a security expert. Rather, he needs to be someone who will report to management and organize the program according to the points described in the WISP.

fieldbrook solutions LLC

Mile 3 – Update Your Technology

Businesses must maintain modern firewalls, plus antivirus and antispyware (or “antimalware” in general)

Note: Having up to date antivirus definitions does NOT mean that you are protected. The software itself must be current as well to protect against the latest threats.

Mile 4 – Identify The PII On Your Network

This may be the most difficult task for larger organizations.

Possible locations of PII:

- Servers (file shares)
- Servers (databases and centralized applications)
- Workstations (My Documents and Desktop folders)
- Laptops
- Home computers (VPNs)
- Email
- Instant Messaging
- BlackBerry and other handhelds
- USB flash drives or portable disks

Mile 5 – Data Encryption

There are many encryption solutions. Which one is right for you?

Hard disk encryption:

- Pro: Generally inexpensive and easy to implement
- Con: Data is secure only as long as it's on the computer

Portable disk encryption:

- Pro: Generally inexpensive and easy to implement
- Con: Data is secure only as long as it's on the computer

Mile 5 – More Data Encryption

Email encryption:

- Pro: Secure and widespread usability/compatibility
- Con: More involved implementation
  and sometimes an inconvenience for users

File encryption:

- Pro: PII is secure no matter where it is located
- Con: May require software implementation
  for multiple, external users

fieldbrook solutions LLC

Mile 6 – Monitoring and Reporting

You must have a mechanism in place to monitor server, firewall, antivirus and other logs on a regular basis.

You must report any breaches of PII directly to the Office of Consumer Affairs and Business Regulation (OCABR) and the Attorney General's office

Mile 7 – User/Employee Education

Your employees MUST be informed and trained on a regular basis of your security policies and procedures.

Have all employees sign Acceptable Use Policies on a regular basis, such as at annual performance reviews.

And Finally, The Exit Ramp

Questions?

Contact Fieldbrook Solutions LLC

http://www.fieldbrook.net

fieldbrook solutions LLC