

THE COMPREHENSIVE INFORMATION SECURITY PROGRAM

MCLE

Navigating the New Federal and Massachusetts Data Security Laws
September 17, 2009

Frank Vincentelli
Integrated IT Solutions
www.integratedit.com

Andrea C. Kramer
Hirsch Roberts Weinstein LLP
www.hrwlawyers.com



Computer System Security

Requirements

Every person and business that owns or licenses Personal Information and electronically stores or transmits such information shall include in its Program a security system covering its computers and networks that includes, at a minimum, the following:

Computer System Security

Requirements

To the extent technically feasible:

- “Secure user authentication protocols”
- “Secure access control measures”
- Encryption
- Reasonable monitoring

Computer System Security

Requirements

And also must

- Have reasonably up-to-date firewall protection, operating system security patches, malware protection, and virus definitions and patches
- Educate and train employees on proper use of computer security system

Computer System Security

Secure user authentication protocols

- Control of user ids
- Reasonably secure method of assigning and selecting passwords
- Control of passwords
- Restriction of access to active users and active user accounts
- Blocking access after multiple unsuccessful attempts to gain access

Computer System Security

Secure access control measures

- Restrict access to records and files containing Personal Information to those who need it to perform their job duties
- Assign unique identifications plus passwords

Computer System Security

Strict access controls

- Application controls: strong authentication and “need to have” access restrictions
- System controls: access privileges and disk encryption

Computer System Security

Encryption

“The transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.”

- All transmitted records and files containing Personal Information that travel across public networks and all data transmitted wirelessly
- All Personal Information stored on laptops or other portable devices

Computer System Security

Hypothetical Case #1:

Joe is a SMB Executive. He forgets his laptop in taxi.

- Laptop has “BIOS” password before booting
- It also has username and “strong password”
- Joe is annoyed at loss of laptop, but feels safe about privacy of his data. Is he right?

Computer System Security

Hypothetical Case #1:

Joe is wrong

- Physical access to a computer almost guarantees any hacker will get to your unencrypted data.
- Hacking does not require a highly sophisticated attacker.

Computer System Security

Hypothetical Case #2:

Joe does not like his company's antivirus program

- Removes it and installs one of his preference
- Company is unaware
- New program fails to update
- Joe believes his computer is protected against viruses and worms. Is he right this time?

Computer System Security

Hypothetical Case #2:

Joe is wrong again!

- Joe's PC can become infected.
- The main company server is now vulnerable to being hacked.

Computer System Security

Lessons Learned

- Actively look for breaches
 - Passive systems no longer enough
 - Security through obscurity is no security
- Test yourself
 - Make sure you find your weaknesses
 - Test often
- Separate “public” servers and “private” data
- Log all access

Computer System Security

Hypothetical Case #3:

A company with an active e-commerce site

- Server is behind a firewall
- Website uses SSL encryption for all data transmissions
- SSL, and ONLY SSL, is allowed from the Internet
- Joe feels good about his server. Can he be 1 for 3?

Computer System Security

Hypothetical Case #3:

Joe just can't get it right!

- Joe's hacked computer (Hypothetical Case #2) can serve as launch pad for attack against server; other attacks exist that exploit operating system vulnerabilities directly.

Computer System Security

Hypothetical Case #4

Joe is very conscious of his company's data, so Joe makes sure everything is backed up daily

- To protect against disaster, Joe diligently manages several weeks' worth of tape sets
- Joe takes one set of tapes to his own house and stores them in his basement.
- Joe's home is broken into...

Computer System Security

Hypothetical Case #4

Meet the new Joe!



Computer System Security

Lessons Learned

- Data should be separated and segregated.
- Data should be encrypted!

The Program

Overall Requirement

Every person and business that owns or licenses Personal Information shall “develop, implement, and maintain” a “comprehensive information security program” (“The Program”)

The Program

General Requirements

- Identify and assess internal and external risks and evaluate current safeguards
- Reasonably restrict physical access to and storage and transmission of Personal Information
- Create employee policies regarding Personal Information, train employees, and establish disciplinary measures for employee violations

The Program

And ...

- Oversee service providers who have access to Personal Information
- Regularly monitor Program, upgrade safeguards, and review security measures
- Respond to and address breaches
- Designate employee(s) to maintain Program

Building the Program

First Steps

Establish an internal data security team

Include someone from Operations, Human Resources, Information Technology, Accounting/Billing, Sales, Legal

Designate one person or more senior employees to oversee and maintain the Program

Building the Program

Hold a Meeting

- Identify every place where Personal Information is kept, the ways the Personal Information is safeguarded in each place, and who has access
- Physically walk around building/facility/office
- Gather all policies and procedures relating to obtaining, sending, storing, accessing, and transporting Personal Information

Building the Program

Types of Information

- Employee information – both current and former
- Client billing/administrative information
- Vendor information
- Information obtained in course of conducting business

Building the Program

What to Consider

- Building security
- Fax and copy machines
- Server locations
- Files at home
- Back-ups
- Old hard drives, servers
- Archives
- Access from home

Building the Program

Review, Revise Policies

- Document destruction and disposal
- Access to archived records
- Access to paper and electronic records
- Disciplinary procedures
- Transmitting or transporting information
- Access to records by terminated employees
- Storage of documents, records, electronic media

Building the Program

Next steps

- Implement electronic security requirements
- Get “RID” of Personal Information
 - **R**edact
 - **I**solate
 - **D**estroy
- Train employees
- Establish schedule for monitoring, testing, and updating Program

Building the Program

Service Providers

Take reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect Personal Information consistent with Data Security Regulations and any applicable federal regulations

Building the Program

Final step

- Enter into contracts with third-party service providers.
- Document whole process, including policies
- Get approval from board, senior management, if necessary