SAMPLE

Professional Organization Security Review

Executive Summary

On *<Dates>*, *Consulting Company* in conjunction with *Management Consulting Company* performed a compliance and security review for *Professional Organization*.

In creating the security review for *Professional Organization*, close attention was paid to the requirements coming into effect under Massachusetts Law 201 RMS 17. These compliance issues need to be addressed on or before March 1st 2010 under the current version of the bill. *Consulting Company* has also included other security best practices which we believe will enhance the security of the *Professional Organization* environment.

The server environment has several major requirements for compliance. It should be one of the first areas addressed. There are non-compliant share permissions, password policies and account practices.

The workstation and laptop environment also will need to be remediated. The requirements will have to be addressed both through the system restrictions and through the clarification of policies and procedures.

The physical environment was reasonably secure for and the majority of transactions, however there is a need for remediation as to how in-coming faxes are handled and stored.

A formal set of policies and procedures must be developed from the ground up. This is the area of greatest concern because focuses on employee training and clear instructions to staff on how confidential information is handled.

Critical Issues:

The following issues must be addressed for compliance purposes.

1. Exchange encryption needs to be implemented
2. Laptops need to be encrypted
3. Share security needs to be reviewed and tightened
4. Computer Archives need to be implemented for long term retrieval
5. Account Management needs to be tightened and implemented
6. Workstation default accounts need to be reviewed for guest and administrator account security
7. Fax Management policy and procedures need to be defined and implemented

Quick Hits for better security and compliance:

These recommendations can be implemented with minimal impact and time.

1. Enable complex passwords
2. Segregate user accounts
3. Tighten and/or disable workstation default accounts
4. Set schedule for regular laptop updates and audits
5. Encrypt Laptop hard drives
6. Set telnet services to disabled
7. Statement of Compliance from service providers having access to confidential material

Scope:

The purpose of this review is to assess compliance with current and upcoming legislation in regards to the handling and storage of personal information, both physical and electronic.

Methodology:

On <Date>a review was performed examining servers, workstations and network infrastructure at *Professional Organization* using industry standard tools. Staff accountant, and Director of Administration were interviewed. The network was also scanned for shared directories and share permissions.

Compliance Requirements:

Core requirements regarding MA 201 Rule 17:

The objective of MA 201 Rule 17 is to protect personal data from security threats, both electronic and physical.

Critical requirements are:

1. Explicit Policies and Procedures regarding the handling of personal information
2. Training of staff in the handling of personal information
3. Physical security of personal data
4. Encryption of electronic data that leaves the immediate secure environment
5. Adequate electronic safeguards to prevent the accidental or intentional unauthorized dissemination of personal information

Personal Information as defined in MA 201 Rule 17:

"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."

Servers and Directory Infrastructure:

Issue: Password complexity is not currently enforced. **This is a compliance issue.**

Problem: Password expirations, reuse, and length are being enforced, but there must be a minimum of a three character complexity rule in place.

Solution: Add complexity to the domain password requirements and train end users on password best practices and methodologies.

Issue: Almost all shares are set for *read/execute* for everyone including finance, customer information, and other confidential information. Certain shares, such as Great Plains, contain confidential information and are at this time fully unrestricted. **This is a compliance issue**.

Problem: Most directories are set for read/execute and several directories under the shares are set for *everyone/full* control. In a few cases, customer and company information is held in shares currently set for *everyone/full* control. Although the *read* attribute is restricted to domain membership, it gives at a minimum read access to all users in violation of the privacy and protection regulations. Some documents in human resources and other locations are password protected, but this is not considered an adequately secure method for protecting personal information.

Solution: Each server will need to be audited, starting with the file servers in order to set the correct level of access and rights in order to secure data. In the instances of human resources, finance, and customer data folders, it is strongly recommended that these shares be restricted and encrypted.

It is also recommended that each functional folder be moved to a private root and share. This can prevent accidental dissemination of information in the event a security setting is misapplied or forgotten.

Issue: Exchange encryption will need to be implemented. **This is a compliance issue.**

Problem: All mail containing protected information must be encrypted outside of the domain environment. The current Exchange implementation cannot check for protected information and cannot prevent the dissemination of protected data through e-mail.

Solution: As discussed in the kick off meeting, plans are in place to implement an edge encryption solution which will automatically detect protected information and will require users to encrypt mail which contains such information.

Issue: User accounts are not segregated. **This is a compliance issue.**

Problem: Old accounts for users are not being segregated to a separate organizational unit in order to deny access to domain resources. Currently old accounts are being disabled in the Users and Boston Users organizational units. These accounts can be re-enabled with full rights restored.

Solution: As employees leave, or as programs are removed from the environment, old accounts need to be moved to a separate organizational unit, disabled, and a policy object will be applied to deny all rights in the environment. The accounts will be held in the directory so that in the event passworded or encrypted information held by that

account can be accessed. The same procedure is also recommended for computers, printers and other infrastructure removed from the environment.

It is also recommended that future program service accounts need to be created and described with the associated program name in a separate service account organizational unit. On two of the current servers there are nearly fifty service accounts at present which cannot be properly monitored due to a lack of description.

Issue: Long term archival storage needs to be implemented. **This is an issue in law.**

Problem: New discovery regulations and financial regulations require a five-year archive of all electronic data regarding tax and human resources records.

Solution: Currently there are daily and weekly backups. It is recommended that a system be implemented for monthly temporary and quarterly permanent data. This can be stored on tape or disk and held at a secure offsite location.

Issue: Expired certificates are present in the environment.

Problem: The domain root certificate used for encryption is currently expired. Until this is renewed, encrypted file shares cannot be implemented. The expired certificate will also prevent policies requiring valid certificates for connectivity from being implemented.

Solution: Renew digital certificates as required and remove all other expired digital certificates from the current directory. It may be necessary to store them in a retired certificates folder.

Issue: Guest accounts are enabled on some servers

Problem: These are known accounts and can be elevated in privilege to access data and programs on individual servers. They are also common pathways for security breaches.

Solution: Disable guest accounts on all systems in the server and workstation environment.

Issue: Telnet services are not disabled on all servers.

Problem: Telnet is an old well-known protocol allowing for remote control of a server. Currently the service is set as stopped but not disabled. This allows an intruder to start the service from a command line and take control of the server.

Solution: Set the service to disabled. It can only be enabled through the services interface and cannot be launched through a command line instruction.

Issue: Domain is a combination of Windows 2000 and Windows 2003 servers.

Problem: Windows 2000 is not considered to be a secure environment due to obsolescence. Security patches are no longer being distributed and the NTLM security protocol is a de facto security access protocol. This means that when a user tries to

connect to the server, the server will first respond with a Kerberos security request but will then automatically fall back to NTLM which is a well documented protocol. The NTLM security hash is commonly tested by hacker tools.

Solution: It is understood that there is a core dependency on the Rapatonni database and interface, It is strongly recommended that this either be upgraded or transferred to a new database platform. The present implementation will prevent migrating to a more current Windows 2008 environment.

Issue: On at least one server, parent paths are currently enabled on the IIS installation.

Problem: A hostile script can be launched affecting the entire server IIS environment.

Solution: Test, and if possible, disable the parent paths option in IIS.

Issue: Many IIS and SQL administrator accounts have weak or non-expiring passwords.

Problem: These accounts will be compromised in a brute force attack. A user with the correct tool set can break in and will have the administrative function on IIS and SQL servers.

Solution: Test and strengthen passwords, if possible. Also set the SQL account password expirations for non-programmatic accounts.

Issue: Shared SQL system accounts are present on all servers.

Problem: These are well-known and documented accounts which allow direct access to database directories and databases. If there is a security breach in one account, many databases will be compromised.

Solution: This cannot be corrected in the current installations without breaking current database access. In the future, non-default accounts should be specified. Include the name of the database and/or application in the account name and description.

Issue: DHCP addresses are being assigned to non-authenticated devices.

Problem: Any device attached to the physical network will receive a DHCP address. This can put the environment at risk through virus attack or an intentional security breach.

Solution: If possible, DHCP addresses should be delivered to known computers and devices. This is not always possible because of old equipment, but should be tested and implemented through policy provided all equipment is capable.

Issue: Currently external connectivity is using single tier authentication only.

Problem: A domain user name and password is all that is required for remote desktop connectivity. Passwords and user names can be cached on remote machines. Without

secondary authentication cached credentials can be used to access the *Professional Organization* infrastructure.

Solution: When the firewall is replaced, it is understood that two tier authentication will be required.

Workstations:

Issue: Laptop hard drives must be encrypted. **This is a compliance issue.**

Problem: Because laptops are leaving the corporate environment, the data is at immediate risk through theft, infection and malware attack. Therefore, it is strongly recommended that all laptop hard drives are encrypted whether or not they directly contain protected information.

Solution: Use a third party encryption tool such as PGP or other whole disk encryption program. Most laptops also have Bitlocker capability. Bitlocker locks the hard drive to the current computer.

Issue: Files can be saved to local directories on workstations. **possible compliance issue.**

Problem: On at least two workstations examined files were being saved to local user directories. In one instance, a subfolder was being shared without permissions applied. Although personal information was not stored on either system, the storage and sharing would not be prevented.

Solution: If possible, local storage should be prohibited through policy. Otherwise personnel policies must be explicit regarding the network storage of confidential information in any form.

Issue: Currently, unprotected shares are being created on user workstations and user home directories. **possible compliance issue.**

Problem: These directories are not properly locked down and have permissions set to *everyone/full control*. In the event of a security breach, such shares can be used to access servers and workstations. They are also vulnerable to accidental loss and/or an elevated privileges attack.

Solution: Only administrators can create shares. Shares must be locked down to access required only.

Issue: Laptops and workstations are not being cleaned before being transferred to new owners.

Problem: There are many directories, user settings and accounts remaining on laptops and workstations which do not belong to current owners. Files and personal information from previous users can go undetected and can result in ongoing infections, keystroke logging or other malware installations.

Solution: When an employee is assigned a workstation, it must be cleaned and freshly installed with only appropriate current account. This will also reduce the likelihood of ongoing capture through hostile temporary files or cookies and other malware.

Physical Security:

Issue: Faxes containing personal information are not always secured. **This is a compliance issue.**

Problem: All confidential and personal information must be maintained in a locked environment when not directly in use.

Solution: A locked cabinet must be available to anyone printing faxes for permanent and temporary storage. This information cannot be left on a desk, inbox or mailbox. The printing of faxes with confidential information should be specified and if possible located in a secure environment.

Policy and Procedure Recommendations

This is an area in which the *Professional Organization* recognizes that substantial progress needs to be made in order to become compliant. Below are recommendations regarding how policies should be created.

Each policy on completion will need to have the following elements:

- A Clear action being addressed
- A Person or group impacted
- Exemptions to the policy
- Result of violation
- An Owner

For the purposes of this review, the action to be addressed will be the primary focus of this section.

1. Protected and Confidential Information access and storage

Physical files containing confidential or protected information must be stored in locked cabinets with access restricted to those with direct administrative responsibility. If confidential information is handled via physical mail, it must be delivered to and from a secure locked location.

Electronic files must be stored in a secure location with access restricted to users requiring access for the purpose of dissemination, distribution or processing.

If protected or confidential information needs to be distributed outside of the domain boundaries, it must be distributed through a secure connection. A secure connection is defined as an encrypted connection and protected transfer site or, if e-mail is required, mail must be encrypted outside of the secure domain environment.

2. Account and access security requirements

Passwords will need to be changed every 90 days.

Passwords must be complex containing three character sets (upper case, lower case, numbers, and/or special characters).

The last password will be remembered and cannot be reused for six password refreshes.

After four incorrect attempts to login, the account will be locked out for a period of not less than five minutes.

For new employees, or employees requiring a new login, an account will be created with a unique user name. On creation of the account, a unique password will be assigned with the requirement that it is changed on first logon. For new employees requiring physical access to protected or confidential information, a key or card key will be distributed and the employee will log and sign for the acceptance of the key or card key.

On termination or retirement of an account, the account will be placed into a retired account organizational unit and all rights will be removed. The retired account OU will actively deny access to domain resources. Any physical access capability such as keys or cardkeys will be retrieved immediately at the time of the terminated employment.

3. Preventive policies

Anti-virus and anti-malware must be installed on all workstations and laptops. Definition files must be updated on a daily basis

The windows firewall or other software firewall must be enabled on all laptops and workstations

Critical files must be backed up on a daily basis and archived on a weekly/monthly/quarterly basis. There must be a test plan for restoration to be executed at least once per quarter.

Firewall firmware must be backed up after each change. All changes must be documented, including risk analysis, and all changes must be approved by the security officer.

4. Laptop, mobile storage and mobile device policies

All laptops must be encrypted.

Laptops must remain as part of the *Professional Organization* domain. Access to customer or other domains must be achieved through a remote client.

Laptop users are responsible for the monthly software update of the laptops in regards to service packs, patches and other security updates.

All mobile storage devices, such as portable drives, USB keys and other writable peripheral devices must be password protected or encrypted if they contain confidential or protected data.

All mobile devices for purposes of accessing and sending mail or file storage must be encrypted or protected through a PIN.

5. Issuance and return of IT equipment

All laptop and workstations will be newly installed on issuance and will be a member of the *Professional Organization* domain. All users will have required rights assigned and the systems will be fully passworded. All standard applications will be installed and configured for use. Additional programs will need to be approved prior to installation by the Security Officer or appropriate manager.

All laptop hard drives will be encrypted when issued

Users are responsible for the removal of all private and confidential files prior to the return of any equipment.

Laptop users will be required twice per year to schedule an update and audit in their assigned office.

6. Training for the handling of confidential and protected data

Each new employee will be trained and instructed in the handling of confidential and protected data.

All new employees or employees with laptops will receive instructions on how to update the laptops with the latest security patches and updates on a monthly basis.

Every employee will need to acknowledge knowledge of and adherence to the above policies in regards to confidential and protected information. This acknowledgement will be in the form of a signed document.

Once a year all employees will need to be trained in the handling of confidential data. This training must be acknowledged by all employees.

7. Procedures in the event of breach

A breach is unauthorized or mistaken access to any *Professional Organization* confidential internal information or its customers while that data or information is in the possession of *Professional Organization* or a *Professional Organization* employee

Such a breach would include a network or system intrusion including virus, malware or attack. It also includes the loss or theft of a laptop.

If such an intrusion occurs, it must be reported on discovery to *Professional Organization* management. *Professional Organization* management will implement notification procedures to appropriate authorities and, if needed, customers. There will also be a causal investigation in order to mitigate future events.

8. Ownership of Security:

There will be a designated security officer responsible for the enforcement and maintenance of the above policies. Any exceptions to the above policies must be approved in writing by the security officer.

Sample Policy

Data containing the following information needs special handling in order to maintain compliance with MA Rules 17.03 and 17.04:

First Name or First Initial and Last Name with:

a. Social Security Number
b. Driver's License or State Identification Number
c. Financial Account Number or Credit or Debit Card Number

Collection of personal information, as described above, will be limited to the minimum required to perform or complete a specific task.

This personal information should be stored on paper or USB drive and held in a secure locked cabinet, held at a secure off site location, or held within an encrypted storage system on a server, workstation or laptop. With an electronic encrypted storage system, explicit rights must be defined specifying which individuals have the rights to view, change, create or delete protected information. This includes both file systems and databases.

This policy will apply to all employees

Director of administration will own and maintain the above policy.