SAMPLE

Preliminary Compliance Review for Generic School

Executive Summary

On <Dates> 2010, *Consulting Company (CC)* in conjunction with *Management Consulting Company* performed a compliance and security review for the *Generic School.*

In creating the security review for *Generic School*, close attention was paid to the requirements of Massachusetts Law 201 RMS 17.03 and 17.04. These compliance issues need to be addressed and remediation documented 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 *Generic School* 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 should also be remediated. The requirements will have to be addressed both through system restrictions and through the clarification of policies and procedures.

The physical environment also has several areas requiring remediation. These include fax and file security.

Generic School has a formal set of policies and procedures which need to be expanded in certain areas to address ownership and the handling of confidential information and procedures to be followed in the event of a breach. Also, there should be a focus on employee training and clear instructions to staff on how confidential information is handled.

Critical Issues:

1. Account Policies regarding complexity must be implemented.
2. Anti-virus policies must be created and enforced. This includes system anti-virus, spam filtering and web host filtering.
3. There must be a written protocol for moving fax documents from the mail area in a reasonable time. Any faxes containing confidential information must be stored in a secure location.
4. Workstations must have screensaver locking implemented in order to avoid systems sitting open overnight.
5. Old User accounts must be segregated and rights removed and denied.
6. The Wireless LAN's are not encrypted or secured.
7. Need to remove shared accounts – Summer accounts.
8. Security on data shares need to be tightened.
9. Backups must be secured through encryption or password.
10. Filing cabinets in all areas are in need of keys.
11. Physical checks are stored in an insecure manner.

12. WISP must specify an owner and a written protocol for notifying authorities regarding a breach.

Quick Hits:

These recommendations can be implemented with minimal impact and time.

1. Enable complex passwords
2. Segregate user accounts
3. Lock filing cabinets and/or desks
4. Set telnet services to disabled
5. Create a lockbox for the Business Office receipt of checks
6. Load Anti-virus on all servers

A request for a Statement of Compliance from service providers having access to confidential material must be on file for each service provider, whether or not they are headquartered in Massachusetts. The review does include a sample letter of compliance which can be sent to each of *Generic School's* service providers including banking, payroll, computer services, document handlers, et al.

Scope

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

Methodology

On <Dates>, a review was performed examining servers, workstations and network infrastructure at *Generic School* using industry standard tools and interviews. The network was also examined for critical security flaws. Business and administrative staff were also interviewed to ensure awareness of the new requirements. Policies and the WISP were also reviewed for compliance.

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: Unsecured wireless LAN access for student and data LAN's

This is a compliance issue.

Problem: Any user can attach to wireless networks in the environment without authentication. This gives full access to all data shares in the environment.

Solution: Enable WEP encryption and keys for all wireless networks.

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 organizational unit. These accounts can be re-enabled with full rights restored.

Solution: As employees leave, or as programs are removed from the environment, old accounts should 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.

Issue: Anti-virus policies and tools must be distributed throughout the environment and tested.

This is a compliance issue.

Problem: Two servers were not running anti-virus. Also, web filtering is not implemented. This can prevent users from inadvertently going to infected web sites or links and infecting the environment. Anti-virus includes system anti-virus software, spam filtering and web filtering.

Issue: Server systems and peripherals are becoming obsolete.

This is a compliance issue

Problem: Three servers are running Microsoft Windows Server 2003 with Service Pack 2. This will be obsolete in January 2011. There is one server running Windows Server 2000, which will no longer be supported in July 2010. The other servers are currently running Windows Server 2003 R2. This will still be supported for at least 18 months. PIX firewall and switches are within the 12 month end of life.

Solution: *Generic School* needs to immediately migrate data from the Windows Server 2000 in order to remove the NTLM protocol from the environment. Planning must also occur as to the upgrade of peripheral devices, including switches and firewalls. Later this year it is recommended that *Generic School* examine current software revisions to prepare a move of the domain to Windows 2008 server.

Issue: Need to segregate Summer accounts

This is a compliance issue

Problem: Shared accounts are not allowed in an environment which stores personal protected information.

Solution: Each summer worker and student must have a unique login and password. At the end of the summer the accounts can be disabled and/or segregated.

Issue: Some shares are open to Everyone - Full Control

This is a compliance issue

Problem: Any user can create folders in and upload files to any network share in the environment. There are folder permissions, but users can fill the drives, create .mp3 libraries, upload network scanners, etc.

Remediation: Shares must be locked down to specific groups, or at a minimum, to authenticated users or domain users. The current configuration opens the environment

to infection. All shares containing confidential and protected information should be moved to the root of the file servers.

Issue: Passwords are required to protect tape or tape backup

This is a compliance issue

Problem: Currently anyone with access to the tapes can restore and obtain protected information. Since backups are file system neutral on restore, a restore to a FAT32 partition would eliminate all file and share level protections.

Solution: Establish either a backup restore or tape password to ensure backup data security.

Issue: Telnet services are not disabled on all servers and workstations

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: It is strongly recommended that files and programs containing protected information be encrypted.

Problem: If a system is compromised from virus or attack, unencrypted information can still be accessed if not encrypted.

Solution: Shares for BlackBaud databases, .csv files and payment information should be encrypted and the encryption key should be exported to an encrypted USB device.

Workstation Infrastructure

Issue: Some users are administrators on their workstations.

Problem: As administrators, users can install executable files, change system settings, change printers, reconfigure their desktops and reconfigure their network. Also, users can then disable anti-virus software, connect to infected websites, download infections, and finally access all system and previous user files on a system.

Remediation: User accounts need to be tested for needed rights. Some software does require enhanced rights on a workstation, but normally, not administrative rights. This will prevent accidental deletion of files, reconfigurations of applications and settings, and will help reduce the number of infected systems in the environment.

Issue: Some users are creating local directories and saving files to the local workstation.

Problem: Saving files locally violates many principals of centralized computing. The first issue is that these files do not get backed up. The second is that the security level of a workstation tends to be substantially lower than on a server. Payroll programs and directories are currently held on workstations.

Remediation: Once administrator rights are removed from workstation users, do not allow users to create local directories on the workstation. Also, ensure that the desktop is part of the profile and is copied to the user directory. For critical applications, such as payroll, ensure directories are locked and encrypted.

Issue: Workstations are remaining unlocked and open when users are not present at their desk.

Problem: When handling sensitive information, it is important to maintain a policy of "in direct control". This refers to the concept that if information is open or accessible, it should be in the control of an employee or process.

Remediation: If a workstation is not in use for 20 minutes, a screensaver should be enabled and password protected in order to secure the computing environment.

Physical Plant

Issue: Filing cabinets need keys

Problem: Users and administrators are filing unused files, however, many filing cabinets do not have keys.

Remediation: Ensure that all filing cabinets containing protected information can be locked and that a key is available.

Issue: Need to remove Social Security numbers and protected information from the emergency forms.

Problem: Only users with a direct job related requirement should have access to protected personal information.

Solution: Create a policy and protocol to control the dissemination and recording of the protected information. If it is not required, ensure a protocol is in place allowing for access when needed.

Issue: Checks are not stored in safe, secure and consistent manner

Problem: Each business group is handling checks in a different manner including storage in unsecured boxes and unlocked desk drawers.

Solution: Establish a lock box adjacent to the business office for the check depositing on a daily basis.

WISP

Issue: Direct owner of security

This is a compliance issue

Problem: The Program Manager is designated as the owner of security in the WISP. The owner must be a named person.

Solution: Director needs to be named as the direct owner

Issue: The WISP requires that violations must be reported to authorities in the event of an intrusion.

This is a compliance issue

Problem: The WISP should specify that the Attorney General and/or local police must be notified in the event of an intrusion.

Solution: If an intrusion occurs in which insignificant data is touched, contact the local authorities, in the event of a major breach, the Attorney General's office must be notified.

Policy and Procedure

Statement of data ownership:

All information transmitted on or stored in any device owned by or connected to the *Generic School* is the property of the school. This includes but is not limited to computers, servers, student workstations, network devices, physical network, printers and audio-video devices. All access to data therefore falls under the IT resource use policy.

Encryption Policy:

All directories containing protected confidential data residing on *Generic School* information technology equipment must be encrypted. The encryption standard is EFS, although other approved third party encryption algorithm is acceptable. There will be an encrypted secure USB drive for recovery purposes. The domain administrator and a designee shall be the recovery agents for the encryption certificate.

This policy applies to all users handling protected personal information per the Written Information Security Plan. Any violation of this policy will result in a review of employee actions and determination of network rights. Punishment will result in a written warning and can lead to dismissal.

The owner of this policy is Jane Doe

This policy will be reviewed annually

Anti-Virus and Anti-Malware Policy:

All systems will run current and registered anti-virus and anti-malware agents. These agents must be set for automatic updates, remain active at all times and be well connected. Administrative and student computers will be examined to confirm the anti-virus configuration at least once per annum and will be subject to spot inspection.

This policy applies to all persons, without exception, having access to *Generic School* resources including educators, students, administrators, contractors, consultants, et al.

If a system is found to be out of compliance all access will be terminated until fully remediated.

The owner of this policy is Jane Doe

This policy will be reviewed annually.

Conclusion

Overall, the changes to be made can be done with minimal cost and impact to the organization. We recommend that *Generic School* begin by following the recommendations listed in the Quick Hits section of the report. The more time-consuming areas to be addressed include enforcement of physical security and the creation of IT procedures to more efficiently handle confidential data. The other challenge will be to create incident reporting procedures.

I would like to thank you for your time and cooperation. It has been a pleasure to work with your school.