Final Report: Security Analysis of the State College Area School District

SRA 221: Section 004-005

Dr. Techatassanasoontorn

Chris M., Ryan G., Joe V. and Natasha B.

Team H1N1 Survivors:

Fall 2009

Table of Contents

Introduction

The client that we focused on was the State College Area School District. After interviewing with their security experts we found that Information security is an essential goal in their organization. Their mission is to establish proficient levels of availability, confidentiality, and integrity for students and faculty in regard to information security. Important student and faculty information should always be secure and not vulnerable to hackers or unauthorized users. For students it is also important that they have limited availability to inappropriate material on the Internet. That is why the School District developed a filter to restrict certain information that could possibility damage a student's education. In this report we will discuss the information security challenges, the Federal Information Security Management Act, categorize information and information systems, select a set of security controls, and discuss the challenges our team faced.

The Federal Information Security Management Act (FISMA) of 2002

The Federal Information Security Management Act is a United States law implemented in 2002 that outlined the importance of information security measures for the nation’s federal agencies. The law has made it mandatory for all government agencies to develop and execute an information security program for all of their information and information systems. The government has hired officials to monitor and inspect agencies’ information security programs annually to report the results to the Office of Management and Budget. This ensures that each federal agency has made it a priority to improve and maintain their information security program. This act advises the head of each agency to apply guidelines and procedures in an economically sound manner to decrease information technology security risks. FISMA was enacted to require organizations with transactions of a Federal nature to the same compulsory criteria expected of Federal agencies.

Department of Homeland Security and FISMA

The Department of Homeland Security’s implementation of FISMA placed it in the middle distribution of rank in comparison to all other government agencies, indicating it is more than possible for the D.H.S. to improve its security measures. The Department of Homeland Security requires all of its subordinate agencies to adhere to FISMA regulations. The regulations contain several subchapters that encompass the following guidelines as listed on the FISMA Web page of The U.S. Department of Homeland Security’s Federal Computer Incident Response Center:

> (A) Assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

> (B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 11331 of title 40, for information security classifications and related requirements;
>
> (C) implementing policies and procedures to cost- effectively reduce risks to an acceptable level; and
>
> (D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented; of information regarding precisely what actions and regulations should be enacted to ensure protection. Content in these subchapters contain information that varies from defining what "information security" is, all the way to delegating the responsibilities of each agency.

The Department of Homeland Security's FISMA standards also state that each agency shall individually evaluate its information security to "determine the effectiveness of such program and practices." An examination conducted by an external auditor is also required to gauge the effectiveness of information security policies (Whitehouse.gov, 2008). After the assessment is complete, the Office of Management and Budget informs Congress of the evaluation results to ensure appropriate protection measures are utilized. The Comptroller General will also report to Congress on the effectiveness of each department and agency.

DHS FISMA Compliance Evaluation

Overall, Department of Homeland Security scored a "Good" rating on the White House's 2008 Fiscal Year FISMA Report (marcorsyscom.usmc.mil, 2008). The four main categories: Effective Plan of Action and Milestones(POA&M), Quality of Certification and Accreditation Process, Completeness of System Inventory, and Quality of Privacy Impact Assessment Process scored “Yes”, “Good+”, “96%-100%”, and “Good” respectively.

Although the Department of Homeland Security scored higher than other government departments, areas in need of improvement still exist. On the CIO report, the only aspect that didn’t have 90 percent or higher in the highest security was the following statement: “The agency applies common security configuration established by NIST to application information systems,” to which the agency scored “Mostly (81-95% of the time)”. The POA&M process is in an authoritative management tool to detail specific program and system level security weaknesses, plus the resources required to implement the plan. Scoring “Mostly” in this regard indicates that while they are not perfect at implementing and pinpointing problems to fix, they are still able to catch the majority of issues and implement fixes. This is still rather high in comparison to other departments. Overall, according to the FISMA evaluations, the Department of Homeland Security obtains a good rating, especially when one observes that the Department of Defense is considered “Failing” in their evaluation.

NIST in Regards to FISMA

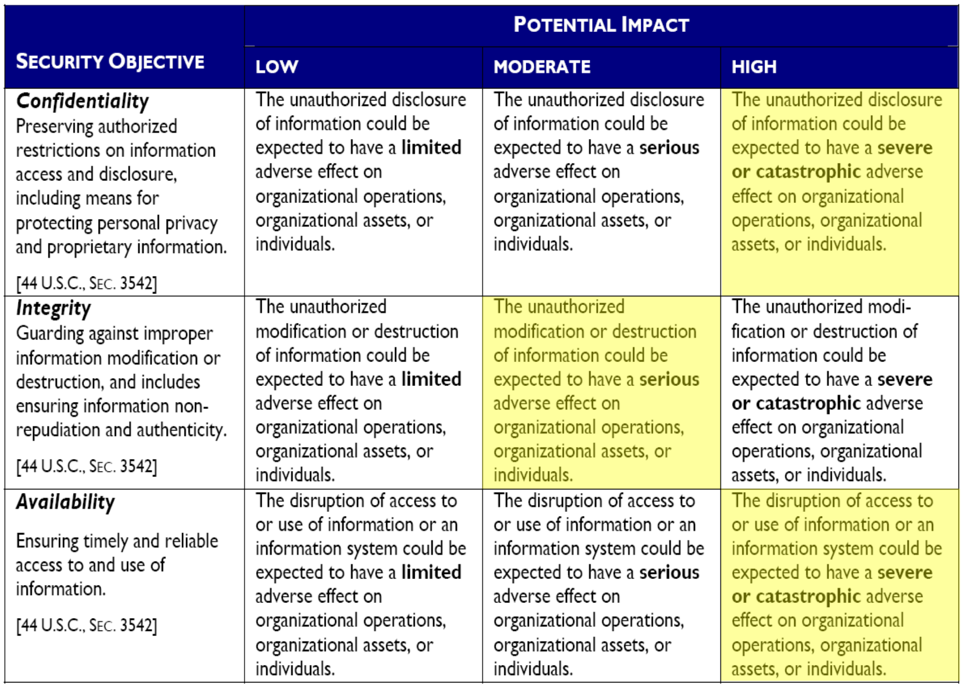
The role of the National Institute of Standards and Technology in regards to FISMA is to set information systems standards and security measures. They set the minimum security standards and select appropriate security controls. NIST is responsible for assessing the security practices of organizations to see if they match those of the standards that NIST has previously established. NIST accomplishes this by doing periodic assessments of risk, which include how much harm would occur if the information or information system were disrupted, had unauthorized access, or were disclosed.

If an organization complies and meets the standards set forth by NIST they are certified and accredited by NIST. FISMA compliance simply means that an organization meets the guidelines established by NIST and FISMA. This includes continuous monitoring overall especially with observing information systems inventory, ensuring systems are categorized by risk level, guaranteeing implementation of security controls, developing and executing a system security plan, and earning certification and accreditation recognition. Once an organization becomes FISMA compliant they have to continue meeting the standards set forth by NIST and FISMA in order to stay compliant. These include annual reports on information systems and security controls. The organization also has to withstand annual testing done on their information systems to make sure all information stays secure.

Categorization of Information and Information Systems

Our client is the State College Area School District. The organization's mission is "to prepare students for lifelong success through excellence in education (State College Area School District Home Page)." The business' aim in regards to security is to focus on maintaining the confidentiality of faculty and student information, while providing accessibility to authorized users. The mission based information type includes personal information and demographics such as social security numbers and student grades. Support and Management data consist of attendance records of students and faculty and emergency dial-outs, such as the electronic initiation of fire alarms.

Source: NIST 800-60 Vol. 1, p. 20 [Areas highlighted for importance]



Security Objective	Potential Impact		
	LOW	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., Sec. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., Sec. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., Sec. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

As shown in the NIST chart above, in regards to the provisional impacts level of the client's information, both 'Confidentiality' and 'Availability' were classified as High Risk categories while 'Integrity' was labeled as a Moderate Risk.

Confidentiality issues include maintaining the security of social security numbers, home addresses and student grades. Each of these issues has a separate impact level depending upon how great a compromise of the information could affect the organization. Social security numbers would be the highest risk in this category where a loss or compromise of their information could cause catastrophic problems for the organization and its students.

Integrity problems are related to the possible alteration of grades or attendance records, which would indicate the system had been compromised. In this area, the organization must implement items such as backups and secure external records to minimize potential loss.

An Availability conflict could cause the computers to become inoperable and security measures could be overridden or operate improperly. The organization must prepare for alternative ways to continue operation if such a conflict was to occur as well as find means of protection to aid in preventing such events. Protective measures such as backup power generators and having trained IT employees to have access to fully resetting the network are a must.

A common threat to an organization is the consequence(s) that could arise from a malicious adversary if he was able to use unauthorized disclosure of information to do some level of harm to agency operations or assets. In this regard, the greatest danger our client faces is identity theft and disclosure of personal information for either employees or students. An example of a past issue was when a student found out about the teacher he was assigned in the upcoming semester before those details were scheduled to be released. Both student and staff records contain sensitive information with addresses, parental contacts, special medical needs and related topics that could violate school and government legislation if released or misused, such as the Health Insurance Portability and Accessibility Act (HIPPA) and the Family Educational Rights and Privacy Act (FERPA).

Preserving the Integrity and Availability of information are also other areas our client must ensure its security measures are prepared to handle. When individuals choose to compromise their Integrity to illegally obtain and or misuse sensitive information, there are adverse effects for those culprits, in addition to the organization overall. If a student gains access to administrator level classification, it would be possible to alter grades and attendance records. Such an incident would only violate school laws and no other types of legislation.

All modifications made are misrepresentations of reality and thereby undermine the integrity of the system and the perpetrators. In regards to Availability, ill intended actions could result in the computers being disabled and the attackers could gain access to unauthorized Web sites. Unlawful access to certain sites would violate the Child Online Protection Act and school regulations. Essentially any serious disruption would prevent business processes from functioning by hindering students' and or faculty members' ability to carry out tasks. (N. Zepp, personal communication, October 27, 2009).

Set of Security Controls

After analyzing the data given to us through the formal interview, we have assessed the requirements of baseline implementations of security controls. Our conclusions are presented below in the form of a chart based off of the NIST Security Control Prioritization Table. Below the chart is an in-depth conclusion of eight of the security controls, with rationale as to why it should be implemented, and how it can be implemented.

	Key	
Priority Code	Sequencing	Action
Priority Code 1 (P1)	FIRST	Implement P1 security controls first.
Priority Code 2 (P2)	NEXT	Implement P2 security controls after implementation of P1 controls.
Priority Code 3 (P3)	LAST	Implement P3 security controls after implementation of P1 and P2 controls.
Unspecified Priority Code (P0)	NONE	Security control not selected.
	Color Coordination by Control Type	
Mission Based		Support Information

	CONTROL NAME	**PRIORITY**		**BASELINES**	
Ctrl. #			**LOW**	**MOD**	**HIGH**
	Access Control				
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
	Awareness and Training				
AT-2	Security Awareness	P1	AT-2	AT-2	AT-2
AT-3	Security Training	P1	AT-3	AT-3	AT-3
	Security Assessment and Authorization				
CA-2	Security Assessments	P1	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-5	Plan of Action and Milestones	P3	CA-5	CA-5	CA-5
	Media Protection				
MP-2	Media Access	P1	MP-2	MP-2 (1)	MP-2 (1)
MP-3	Media Marking	P1	Not Selected	MP-3	MP-3

As stated where we analyzed the potential impacts of each security objective, both confidentiality and availability are rated as ‘high’ and integrity was rated as ‘moderate’. Below are eight of the security measures the organization can take to improve security and decrease the chances of high risk security failures from happening.

The rationale for each individual security control was carefully thought out on how and why it should be implemented. Each individual security control is divided into three sections. The first is “baseline security controls” which states the bare minimum that should be implemented by the high school. The next section is the rationale, which explains why these measures must be taken. The final section discusses how the “baseline security controls” can be implemented. The first four listed below apply to mission-based information while the four afterwards are for support information.

Access Control Policy and Procedures

Security Objective(s) Affected: Confidentiality, Availability, and Integrity

Individual Risk: High

Baseline Security Controls:

A periodic development, update and dissemination of a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

Rationale

This is the benchmark for the majority of access control security. With this instated, the organization can begin to filter between authorized and unauthorized users, which allows for the organization’s primary mission of education to continue.

Implementation:

The access control policy and procedures should be a written document that is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The document is also able to be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, or for a particular information system, when required.

Account Management

Security Objective(s) Affected: Confidentiality and Integrity

Individual Risk: High

Baseline Security Controls:

The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts at least annually.

Rationale:

Account management will lessen the chance of accidental exposure of sensitive information to unintended users. With proper account management, users who do not need to see sensitive information will not be able to.

Implementation:

Authorized users of the information system must be identified along with each individual access right and privilege. Information should only be granted when it meets one or more of the requirements below:

1) A valid need to know or need to share basis – determined by assigned duties

2) Intended system usage – proper identification must be required to approve or establish any system accounts. All unnecessary accounts must be disabled or removed.

In order to enhance security, the following measures should be implemented as well.

1) Employ automated mechanisms to support the management of information system accounts.

2) Automatically terminate temporary and emergency accounts after a set time

3) Automatically disable inactive accounts after a set period of time

4) Employ automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.

If all of the above actions are implemented, account management will become a highly secure area for the organization.

Media Access

Security Objective(s) Affected: Confidentiality

Individual Risk: High

Baseline Security Controls:

The organization restricts the information system media to only authorized individuals.

Rationale:

The reason that the media access is needed to improve the security of this organization is because there is a big need for restriction of information media including digital media. Within a school environment there are a lot of students and faculty who use external hard drives, flash drives, video disks, compact disks, and diskettes. The control will also be put in place for mobile devices. The reasoning for this control is because students and faculty members who do not have authority should not be able to store or import information via these media devices because it could cause security complications. The problems caused could be the transportation of malicious materials like viruses or other malware. Restricting this will eliminate this possibility.

Implementation:

The goal in the implementation of media access is to provide a learning environment that can be enhanced by media but to restrict media storage to only authorized users. To complete this task the organization will have automated mechanisms that work to restrict access to media storage areas and to review access attempts and access that was given. This restriction improvement can be put in place only at assigned large media storage areas in the organization and not at every single location.

Media Marking

Security Objective(s) Affected: Confidentiality

Individual Risk: High

Baseline Security Controls:

This organization will label information system media putting limitation on certain content. Materials that are considered to be inappropriate for students will be marked with a label that will make the system restrict students from viewing the material. For example, there will be a list of inappropriate words that can be typed into a search engine or as a domain name. This is to ensure that if a user inputs one of these words they will be restricted from viewing the media.

Rationale:

The reason that all information system media should be labeled is because there is a lot of media that would not be suitable in a school environment. Student's main goal is to learn and anything that could disengage this goal or restrict them from continuing their education should be blocked. Students are minors and by law they are not old enough to view adult material. Therefore, any illegal media should be restricted as well.

Implementation:

As mentioned above, all content will be labeled so some media will be deemed accessible and some will be restricted. The material that will be restricted will be based on the organizations policies and procedures. Basic policies will not allow any pornographic, violent, or any racially crude material to be accessed. These inappropriate materials will be labeled inaccessible so when a user tries to access them by inputting a key word or phrase, the system will check the list of inappropriate words and if there is a match they will not be granted access. Other media that is noted by the FIPS199 security categorization must also follow the regulations determined by said document.

Security Awareness

Security Objective(s) Affected: Confidentiality, Availability, and Integrity

Individual Risk: High

Baseline Security Controls:

The organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and at least annually thereafter.

Rationale:

Security awareness allows the non-technical employees and clients of the organization to understand the security implementations that affect them as well as how to avoid causing security issues for the organization.

Implementation:

The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access. The organization's security awareness program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in SP800-12. A few of the main requirements in C.F.R 930.301 are:

1) All users of Federal information systems must be exposed to security awareness materials at least annually.
2) Executives must receive training in information security basics and policy level training in security planning and management.
3) Program and functional managers must receive training in information security basics

Security Training

Security Objective(s) Affected: Confidentiality, Availability, and Integrity

Individual Risk: High

Baseline Security Controls:

The organization identifies personnel that have significant information system security roles and responsibilities during the system development life cycle, documents those roles and responsibilities, and provides appropriate information system security training.

Rationale:

Training personnel that have roles within the organization in regards to security will create an overall more secure environment. It also allows for quicker and more appropriate responses to security issues that occur later in the organization's life.

Implementation:

Training should be implemented during the following occasions:

1) Before authorizing access to the system or performing assigned duties

2) when required by system changes; and

3) After a set interval - that is determined by the organization

In addition, the organization provides system managers, system and network administrators, and other personnel having access to system-level software, adequate technical training to perform their assigned duties. The organization's security training program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in SP800-50 (as stated above).

Security Assessments

Security Objective(s) Affected: Confidentiality, Availability, and Integrity

Individual Risk: High

Baseline Security Controls:

The organization conducts an assessment of the security controls in the information system at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Rationale:

Requiring an assessment at least annually to ensure that controls are implemented correctly will allow for a reduced amount of security flaws and problems. All aspects of security are improved (more significantly when conducted more than once a year) when they are checked as the organization has the ability to find and fix the problems before they can be used by unauthorized or unintended users. This security measure is also a required action from FISMA.

Implementation:

To satisfy the annual FISMA assessment requirement, organizations can draw upon the security control assessment results from any of the following sources:

1) Security certifications conducted as part of an information system accreditation or reaccreditation process

2) Continuous monitoring activities

3) Testing and evaluation of the information system as part of the ongoing system development life cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness).

Organizations should also use this to meet OMB's policy of assessing a subset of security controls. This subset is based upon:

1) The FIPS199 security categorization of the information system

2) The specific security controls selected and employed by the organization to protect the information system

3) The level of assurance (or confidence) that the organization must have in determining the effectiveness of the security controls in the information system.

Plan of Action and Milestones

Security Objective(s) Affected: Confidentiality, Availability, and Integrity

Individual Risk: High

Baseline Security Controls:

The organization develops and updates periodically (period determined by the organization), a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

Rationale:

Keeping a plan of action and milestone for the information system will allow for the improvement of the overall organization's security and reduce infringements upon their policy.

Implementation:

The plan of action and milestones is a key document in the security accreditation package developed for the authorizing official and is subject to federal reporting requirements established by OMB. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. SP800-37 provides guidance on the security certification and accreditation of information systems. SP800-30 provides guidance on risk mitigation.

Conclusion

Our security recommendations are to be used as a basis to aid the organization in implementing new security controls and improving their old security. As provided by our analysis above, the key areas to implement high security are the Availability and Confidentiality portions of the organization. It is important to ensure that these areas are highly secured due to the highly problematic events that could occur of such information was lost or stolen. By following the actions provided within this document, and making the suggested improvements, the organization can become a lot more secure area for its clients, students, and faculty.

Works Cited:

Fiscal Year 2008 Report to Congress on Implementation of the Federal Information Security Management Act of 2002. (2008). Retrieved October 19, 2009, from http://www.whitehouse.gov

Federal Information Security Management Act (FISMA). (2002). Retrieved October 19, 2009, from http://www.marcorsyscom.usmc.mil

SP800-53rev2. (2009). Retrieved November 19, 2009, from http://ia.digipro.com/ia/SP800-53rev2?control/CA-05

National Institute of Standards and Technology. (2007). *Recommended Security Controls for Federal Information Systems.* Gaithersburg, MD: Information Technology Laboratory.