Data Security Guidelines for Student Information Systems

John Escalera

A Prospectus Presented to the Information Technology College Faculty
of Western Governors University
in Partial Fulfillment of the Requirements for the Degree
Master of Science in Information Security and Assurance

1/17/2012
Abstract

The purpose of this study is to create a set of governing rules, or best-practices, which can be applied to any database, computer system, or related software application that deals with student information. Specifically, data housed at an educational institution and shared with 3rd party researchers will be evaluated. I will attempt to investigate what I believe to be a very relaxed atmosphere, and in some cases non-existent basic security policies, in organizations that utilize large amounts of sensitive student information. These best-practices will be aligned with existing state/federal laws related to the protection of sensitive student information such as the Family Educational Rights and Privacy Act (FERPA), the California Educational Code, and in some case the Health Insurance Portability and Accountability Act (HIPAA).

In carrying out this study I will utilize my experience in the field to derive a set of guidelines that address major areas of concern regarding sensitive student information. These areas, though they should be considered untested hypotheses for the purposes of this study, are, in reality, shaped by my extensive experience in the field. I have a strong foundation for these best-practices based on personal experiences in dealing with data related to students and, while I could create an effective set of guidelines using only personal experiences, I will attempt a more scientific, and simultaneously more thorough, approach. I will be selecting a focus group consisting of a set of randomly selected personnel in districts in California, with whom I transfer and receive student data on a regular basis, then create and administer a security survey to the chosen personnel.

The results of this survey should help me to create a more complete set of guidelines. Though I will attempt to create a rigorous set of guidelines, special attention will be placed on those areas which the survey results point to as the most commonly lacking areas of data
security. The outcomes of this project will be a thorough understanding of commonly misunderstood, misinterpreted, or simply ignored areas of data security in student information systems for the reader and a set of guidelines or best-practices that can be extracted as a standalone document and distributed to any organization that utilizes student data and is subject to state/federal student privacy laws.
Table of Contents

Introduction........................................................................................................................................5

Project Scope ....................................................................................................................................5
Project Rationale.................................................................................................................................6
Problem Summary ..............................................................................................................................6
Problem Background ..........................................................................................................................7
Need for the Solution ...........................................................................................................................7
Reason for Approach ..........................................................................................................................8
Prospectus Organization ...................................................................................................................9
Problem Statement .............................................................................................................................9

Background Information ....................................................................................................................9
Causes ................................................................................................................................................10
Business Impacts...............................................................................................................................11
Cost Analysis ......................................................................................................................................12
Risk Analysis ......................................................................................................................................12
Assumptions.......................................................................................................................................13
Limitations ..........................................................................................................................................14
Technical Terms................................................................................................................................14

Technology Solution ........................................................................................................................15

Business Drivers ..............................................................................................................................15
Justification.......................................................................................................................................16
No Solution .......................................................................................................................................16
Solution............................................................................................................................................17
References..........................................................................................................................................18
Introduction

As the political focus of “what’s going wrong” in our schools intensifies the need to utilize student information for statistical analysis will increase accordingly. This will, in turn, lead to an increase in the release of sensitive student data to 3rd party organizations such as researches, evaluators, and other statisticians. This study is based on the hypothesis that both these 3rd party organizations and the original owners of the information (schools, district offices, county offices of education, and state departments of education) often lack the resources to properly secure this student information.

Project Scope

The security guidelines, which are the expected outcome of this study, may address any system that stores, transmits, or receives student information but will be focused specifically on the sharing of data between educational institutions and 3rd party researchers. This will include storage mediums such as commercial student information systems, customized data-warehouses, and personal computers storing flat-file information utilized by each group mentioned above.

The definition of the ‘student’ or ‘school’ will be confined to the Kindergarten through 12th grade ecosystem. While the guidelines will be generic enough to be useful in colleges and universities, these organizations are generally staffed with more qualified personnel (as compared to K-12 schools) and generally have their own security policies established as well as security awareness training programs.

This study will not address security topics that deal with securing an individual workstation, a specific type of information medium, or any specific type or configuration of a network unless it specifically relates to student information systems. These areas are part of the greater realm of information security and are beyond the scope of this study.
Project Rationale

The rationale for this project stems from my personal experience dealing with student information and, consequently, my concern with the handling of data security. I believe that the lack of focus on information security, which I feel exists in the education sector, is based on the mistaken assumption that student information can’t actually be classified as ‘sensitive’ unless it falls under some existing privacy law such as HIPAA, FERPA, or the California Education Code.

While this may be true in part, the fact remains that very few individuals that are expected to secure student data are familiar, or even aware, that there are existing regulations to protect student information. Compounding the problem is the reality that smaller organizations do not have staff members with the skill set required to read, understand, and apply existing regulations. It is my desire that this study will produce a set of guidelines that will help these individuals meet a minimum set of security requirements.

Problem Summary

While laws exist to safeguard personally identifiable student information, the reality is that many small to medium sized schools and districts do not have the budget to employ a staff member qualified to create and maintain security policies and procedures. This duty normally falls to the local computer technician, who may only be qualified to troubleshoot hardware, or, when the school uses contractors for their hardware needs, these duties fall to other staff members such as counselors, administrative assistants, or vice-principals.

Conversely, when a district is large enough to devote an entire team to information security, this team usually gets bogged down with securing the network or individual...
workstations and places the task of securing student information into a low priority queue. It has been a common theme throughout my work in the field that the resources devoted to student information security are little to none, at some times by necessity and at other times by choice.

**Problem Background**

Although the field of student information is ubiquitous, as everyone has been through a school at some point and their personal information has been collected, it is often overlooked based on the perception that there is no direct correlation to breaches in student data, at least for students prior to the collegiate level, and financial loss. This has led to a lack of resources applied to the safeguarding of student data and the mistaken belief that most student information isn’t considered ‘sensitive’ unless it contains a social security number. Because most student information is presented with only a local student identification number it is often assumed that it does not fall under existing privacy laws.

The reality is that in order for this information to be useful, especially to 3rd party evaluators and researchers, it must be combined with some sort of matching file such as an SSN-to-Student ID table. The process of tracing these student identifiers back to sensitive data becomes trivial. Therefore, for the purposes of this study, I will make no distinction between sensitive and non-sensitive information as most non-sensitive information will inevitably lead a motivated individual back to sensitive information.

**Need for the Solution**

While the existing state and federal laws are clear in their expected handling of student information the reality is that current education staff is under-equipped to ensure proper data
Data Security Guidelines for Student Information Systems

security. In cases where the staff members for a particular organization are indeed certified to secure student data they are often left with few resources to devote to the topic. In cases where an organizations staff members are unqualified for this task they require guidelines that are less technical in nature in order to adhere to existing privacy laws.

Both types of staff, qualified and unqualified, would benefit for a guide or checklist of items that would make them compliant with existing state and federal privacy laws concerning student information. For the former it would serve as a checklist to ensure they are meeting the minimum requirements and for the latter it would serve as guide to meeting these requirements.

**Reason for Approach**

While writing a thorough paper identifying the problems, current procedures, and presenting a detailed solution is necessary, the fact remains that this study, in its entirety, will not be any easier for unqualified staff members to consume than reading through the existing state and federal privacy laws mentioned previously. The outcome of this study, as stated previously, is a set of guidelines that may be used as a checklist or guide by any organization wishing to comply with existing privacy laws.

In addition, while I feel that my experience makes me more than qualified to identify most areas of concern and address them accordingly, I am also aware that this study will benefit from input by colleagues of mine who are expected to deal with student information security, whether qualified or not. Therefore, the survey described above will serve to supplement my set of guidelines by adding topics that address any lack of experience or foresight on my part.
Prospectus Organization

The remainder of this prospectus will be presented in two major parts, the problem and the solution. Each major part will be divided into several subtopics that present the topic in an organized manner. The first part, the Problem Statement, will consist of background information about the problem, causes of the problem, business impacts, a cost analysis, a risk analysis, assumptions about the problem, limitations, and a list of technical terms.

The second part, the Technology Solution, will lay out my recommendations for solving the problem described and will consist of subtopics such as business drivers, a justification for the solution, the effects of not implementing a solution, and a description of the solution.

Problem Statement

Background Information

Every young American attends school, whether public or private, from approximately 5 to 18 years of age. During this time a wealth of information is collected from or for each student including, but not limited to date of birth, social security number, medical information, standardized test scores, and mental health information.

Although there are existing state and federal privacy laws governing the storage, use, and distribution of this information, several causes, which shall be described in the following section, contribute to the lack of resources applied to the area of student information security. This lack of focus on student information security is based on the assumption that unlike adult students, such as those in colleges and universities, younger students are not as exposed or vulnerable to the malicious acts that are often the result of security breaches such as identity theft.
Specific excuses for the lax security include such responses as “these kids are too young for someone to open a credit account in their name”, “their medical records aren’t a big deal, it’s just immunizations and such”, and “their standardized test scores can’t be used for any malicious purposes”. However, with enough motivation any of this information will lead a motivated individual on a path to a wealth of private information.

Causes

The root cause for the problem described, particularly in the public school system, is a lack of resources. These resources can be thought of as qualified security staff, proper software solutions, and the creation and maintenance of the district security policy. However, all resources mentioned share a common root, funding, which eliminates the need to discuss them specifically. Well-funded schools and districts generally have staff qualified to implement the appropriate security procedures as well as staff members that have a specific set of job duties so that at least one staff member is specifically tasked with the securing of student information security. However, as mentioned previously, the reality is that individuals who are considered the owners of tasks related to securing student information are often assigned additional tasks that eventually supplant their original responsibilities.

Where schools and districts are under-funded the problem is compounded by the practice of randomly assigning the task of securing student information to a local computer technician, an administrative assistant, or to an administrator such as a vice-principal. In extremely small districts, such as in rural areas, a district may only consist of one school and 3 staff members where only one of these staff members is college educated. This makes it extremely unlikely
that anyone will ever attempt to read and understand existing privacy laws as they relate to student information.

**Business Impacts**

Perhaps the most important impact this problem has, at least from the point of view of the organization from which the data originates, is the violation of state or federal privacy laws as the result of a data breach. While this study is intended to focus on these laws, which affect the educational institutions and 3rd party researchers alike, there are consequences for the individuals whose private information is released.

These consequences may include identity theft, stalking (both cyber and physical), misuse of school schedules during custody battles or kidnapping attempts, the misuse of data for political attacks (i.e. the use of graduation data, aggregated in a specific way, to contradict graduation rates published by an educational institution), the dissemination of mental health or medical information that leads to classroom safety concerns, and the release of citizenship status that may open the door for discrimination.

The consequences described in the prior paragraph, although outside the scope of this study, directly correlate to business impacts that are within the scope of our study. There are costs associated with a breach in security, such the cost of performing audits and notifying individuals of the security breach, as well as the cost of litigation that generally follows such an event.
Cost Analysis

The desired outcome of this study is the creation of a set of guidelines that can be applied to an existing educational infrastructure, without needing to be interpreted by qualified personnel, and will adhere to existing state and federal privacy laws. These guidelines, however, will not be suggesting anything that would require the purchase of any software, hardware, or hiring of additional staff nor do existing state and federal privacy laws suggest this. While it may be suggested that, if the organization feels the need to spend on a solution, money should be spent on qualified staff, one of the requirements of our guidelines is that they should be simple enough to be implemented by the existing staff.

Therefore, the cost to implement this solution, in terms of dollars, is minimal. It will require resources, which may converted to dollars, that include the time necessary for staff to reach and understand the guidelines, the time needed to implement the suggestions of the guidelines, and the time necessary to make changes in existing policies.

Risk Analysis

Perhaps the largest exposure to risk, aside from doing nothing, is failure to maintain and update the guidelines. Having a set of guidelines, and implementing them, may instill a false sense of security into an organization and result in the organization never revisiting this topic to ensure that new and existing staff are aware of the guidelines and procedures. In addition, the existence of our guidelines does not ensure that all staff members are aware or familiar with them and, therefore, it is unlikely that any 3rd party which requests sensitive data will be required to adhere to these guidelines.
Because our guidelines will be based on existing privacy laws it is likely that they will become outdated, at least somewhat, within a few years. Changing laws and regulations present a major challenge to our proposed guidelines and increase risk exposure. One final area of risk, though not as common as those already discussed, is the pressure from superiors to circumvent policy in exchange for efficiency. It is not uncommon for a superior to ask a direct-report to ignore certain security policies, such as a policy prohibiting the transmission of student data over email, in order to avoid having to set up a secure transfer.

**Assumptions**

As we consider how these guidelines would be applied to an organization, and how we deal with the limitations of the organization, it becomes clear that we are assuming the problem is based on a lack of resources, such as time, money, and the existence of qualified staff, when the problem may be attributed to indifference. It may well be the case that an organization has a staff that is competent enough to bypass our guidelines and simply study existing state and federal privacy laws but that simply has no desire or directive to do so.

An additional assumption is that it makes sense financially to implement these guidelines. In a previous example I described a rural district consisting of one school and 3 staff members. If, for example, the district had a student population of 20 students a risk-analysis might conclude that it would be less costly to prepare for the costs associated with a security breach than to attempt to prevent it based on the likelihood that anyone would ever attempt to steal information.
Limitations

The problem described will be limited to school and districts within the state of California. Though the problem, and its proposed solutions, is generic enough to describe a larger geographic area this study, specifically when we discuss state privacy regulations, should be confined to the state in which the author currently resides. As described in the Scope section of this prospectus, this study will also be limited to the K-12 ecosystem and to the public school arena. It should also be noted that although it may not be stated in the guidelines, some of the guidelines will be included specifically to address the sharing of data with outside entities such as 3rd party evaluators, statisticians, and researchers.

Technical Terms

*Educational Code* – For the purposes of the study, the portion of California state law dealing specifically with laws and regulations in education.

*FERPA* - Family Educational Rights and Privacy Act (FERPA)

*HIPAA* - The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

*K-12* – Elementary, middle, and high schools including grades 0 to 12

*Non-sensitive Information* - Any piece of information that cannot be used directly in a malicious manner for the purposes of violating privacy.

*Qualified Personnel* – Any staff member certified, or otherwise qualified by educational achievement, to understand and implement a minimal form of security policy.
**Sensitive Information** – Any piece of information that can be used in a malicious manner for the purposes of violating privacy.

**Unqualified Personnel** - Any staff member not certified, or lacking the education, to understand and implement a minimal form of security policy.

---

**Technology Solution**

**Business Drivers**

As described previously, the problem may be viewed from two angles. The first is the educational instruction acting as the guardian of this data whose primary concern is eliminating the violation of privacy laws and the release of sensitive student information that might be used for malicious purposes. Such breaches of security underscore the primary business drivers for our proposed solution which are, as previously mentioned, the violation of existing laws, reducing the cost of recovery, and reducing the likelihood of legal action by the victims of a breach.

For 3rd party evaluators, researchers, and statisticians the primary business driver is proof of integrity. When the 3rd party can prove that their security policy matches or exceeds that of the educational organization it is less likely that they will be suspected to be the root cause of a security breach and subsequently blamed for a loss of data. In addition, because 3rd party evaluators are generally private businesses, a loss of clients could result from any negative press resulting from a breach if blame is placed on the business.
Justification

With respect to the educational institution, it is our assumption that they are lacking sufficient resources, specifically money, already and that they cannot afford the additional cost of auditing, recovery, notification, and litigation associated with the loss of data. Furthermore, malicious use of private data may have an effect on the trust that students, current and future, and parents have in the organization.

Similarly, for the 3rd party evaluators, researches, and statisticians, the cost of losing clients due to a security failure and the change of public opinion or confidence in your company could be enough to destroy even longstanding business relationships. While it would be infeasible for these entities to adhere to the specific guidelines of each of their clients, using a recognized set of best-practices, such as those that are the stated outcome of this study, would allow a 3rd party to establish a baseline to guard against the possibility of being blamed for a security breach.

No Solution

Sadly, in many cases the problem is, and will likely continue to be, unaddressed. The ramifications of not addressing the situation may include litigation by victims, loss of contracts for 3rd party researches, malicious use of the data for identity theft and other identity related crimes, increase costs to an organization to cover the costs of a security breach, and in some cases criminal prosecution.

In most cases, the benefit of implementing a solution far outweighs the costs associated with doing so. With the guidelines that will be produced as a result of this study there should be
no reason for any educational institution to continue without at least a minimal set of security policies. Essentially, the aim of this study is to make ‘no solution’ unacceptable.

**Solution**

The first focus should be to become compliant with existing state and federal privacy laws. While it can be argued whether or not they are the most important, ignoring these regulations exposes an organization to the greatest amount of risk. Compliance with these regulations will simultaneously make you more secure and less vulnerable to litigation.

Having its own security guidelines, or in our case a set that’s borrowed but an extension of the existing laws, may help an organization decrease its legal risk by providing a document that may be used during legal proceedings.

This solution will be concise, easy to understand, easily implementable, provide for a low cost implementation, and will be shareable with any 3rd party organization with which data must be shared.
References

California Education Code, § 49073-49079.7.
