FUTUREX

WHITEPAPER

The Role of Data Security in Educational Institutions

The information provided in this document is considered proprietary and confidential.

TABLE OF CONTENTS

THE ROLE OF DATA SECURITY IN EDUCATIONAL INSTITUTIONS

Educational organizations represent one of the largest institutions across the world. As such, they are responsible for a vast amount of sensitive data, and as the number of students attending institutions of higher education swells across the country, that data amount is increasing in kind. From faculty research information to the social security numbers of students, the security of this data is paramount to the success and reputation of these institutions. By implementing hardware-based security solutions, schools and universities can gain the upper hand in protecting data and meeting regulatory standards.

INTRODUCTION

In February 2014, hackers succeeded in stealing more than 300,000 records of University of Maryland staff, faculty, and students.[2] Later that same month, a breach at Indiana University compromised the personal data of more than 146,000 students and recent graduates.[1] Names, social security numbers, university ID numbers, addresses, and birthdates belonging to these individuals were all exposed, a veritable goldmine for those seeking to sell personal information on the black market.

At Virginia Tech in 2013, 145,000 records of university job applicants were leaked due to human error, with a server full of the data left without proper security precautions.[4] Information ranging from driver's license numbers to conviction data was left exposed for almost a month before university officials became aware of the breach.

Breaches are not just limited to the higher education sector. Independent school districts are also targeted by hackers, with children at risk of having their personal data exposed. An administrator's laptop and unsecured external hard drive stolen in January 2014 held approximately 14,000 records of students at Midland Independent School District, containing mainly social security numbers.[5] Beyond incidents similar to Midland ISD, breaches can include data such as disciplinary records or medical history, information that can negatively affect a child for years to come if spread on the internet.

In addition to personally identifiable information, both private schools and universities must protect the financial data of those paying for the education. Servers full of financial information will be tested for any weakness by those who would use that data for nefarious purposes, so ensuring proper security protection is in place is crucial.

Without a doubt, data breaches both at the higher education and independent school district levels are of serious concern. Data breaches can do real harm to the credibility of any institution, as

individuals weigh whether they wish to attend a university or school with a history of leaking sensitive information. Beyond the intangibility of reputation loss, data breaches represent very real cost. According to a Ponemon Institute study, that cost averages $111 per lost record in the education sector[3], a sobering figure considering the sheer volume of records processed by these institutions.

Regardless of the motivation behind a security breach – obtaining valuable data for sale, espionage, financial fraud, cyber warfare, or sabotage – it is in the best interests of academic institutions to protect themselves, their communities, and their data from a myriad of security threats that exist in the education sector. In addition to thwarting potential breaches and attacks, protective measures help establish compliance with industry regulations.

REGULATIONS

Data privacy and security practices are governed by a number of regulations intended to protect data subjects and institutions from breaches and other security threats. Data collected and stored by educational institutions are subject to rules and regulations stemming from a variety of agencies, acts, and industry groups.

FERPA

Chief among these regulations is the Family Educational Rights and Privacy Act (FERPA), which applies to all schools that receive funds from the U.S. Department of Education. Institutions that regularly violate FERPA are at risk of losing this funding. FERPA concerns itself primarily with the privacy of academic records.

FERPA allows students over the age of 18 to seek access to their academic records and to contest those records. To provide this accessibility to students (and to maintain strict privacy of those documents throughout information systems) requires a notable degree of flexibility and security from academic institutions.

HIPAA

All healthcare organizations are subject to the Health Insurance Portability and Accountability Act (HIPAA), whether they are a globally recognized hospital or a small elementary school health facility. Health clinics for universities and district level schools must treat student records with the same level of care as regular healthcare organizations' data.

PCI DSS

Any educational organization that processes card payments, from tuition to private donations, is subject to compliance from the Payment Card Industry Data Security Standard (PCI DSS). This standard ensures that cardholder data is kept secure at all times, reducing the likelihood of a financial data breach.

ABOUT FERPA

FERPA regulates a wide range of academic records, including:

- Transcripts, exams, and papers
- Database systems
- Class schedules
- Financial aid records
- Financial account records
- Disability accommodation records
- Disciplinary records
- Unofficial files such as emails, photographs, and hand-written notes
- Records publicly available elsewhere or that the student has publicly disclosed

This data can be tokenized and stored in a secure vault to reduce compliance scope.

To learn more about FERPA, visit:http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Other state, federal, and industry regulations affect the way data is secured in educational organizations, such as the Fair Credit Reporting Act and FISMA, among others. In addition, research funded by specific grants may be subject to the security-related rules and regulations of the grant-providing institution.

The result of regulations aimed at data security optimization in the education sector is an increased need for systems that thoroughly protect data while maintaining accessibility for authorized parties. In preventing breaches, complying with industry and governmental regulations, and meeting the needs of the academic community, data protection solutions must provide industry-leading security features as well as functional accessibility for authorized users.

OPPORTUNITIES FOR PROTECTION AND PREVENTION

The IT departments of academic institutions are faced with some unique data security challenges. The following examples show just a few of the ways data breaches can occur and, more importantly, be avoided.

ACADEMIC RECORDS

The most high-profile breaches in the education sector are those that affect what FERPA classifies as academic records: students' personal information, such as social security numbers, names, and addresses. The exposure of this information can be expensive and difficult for educational institutions to remedy. To prevent such compromises, it is critical for institutions to implement a security solution that protects these documents from unauthorized view.

Tokenization is an alternative to in-the-clear storage of information that maintains data usability but greatly reduces the risk of sensitive information being accessed by unauthorized parties. Tokenization masks only data deemed sensitive by replacing it with an identifying text string ("token") generated by a hardware security module (HSM).

HSMs are dedicated cryptographic appliances that protect sensitive data through physical security measures, logical security controls, and strong encryption. To "detokenize" information, the token is sent to the HSM, which then returns the clear data safely and securely. Tokenization offers organizations the security of hardware-based encryption while retaining near-full usability of the original data.

For information not likely to be needed on a regular basis, such as the personal information of students who have graduated in the past or faculty are no longer employed at the institution, HSMs provide a way to store that data in secure manner, encrypting it within a FIPS 140-2 Level 3 validated attached server for high volume storage.

RESEARCH DATA

Conducting research is often an expensive and time-consuming enterprise. For this reason, research results are valued highly not only by those who sponsor and conduct research, but by those who mean to illicitly obtain such data. Unauthorized access of research data can be a means of bypassing significant investments in research; a method of corporate, government, or institutional espionage; and a possible instrument of sabotage. As a result, protecting research data is of paramount importance to educational institutions and the governmental and fund-awarding bodies that support them.

Ensuring that research data is authentic – unmodified and original – is essential to those engaged in the research process. Implementing digital signing mechanisms for research data ensures authenticity while encrypted storage platforms establish centralized repositories for housing this data. Certificate authority technology offers signing and

validation of files, allowing institutions to verify authenticity before encrypting the data for storage or transmission to partner institutions.

Loss of research data, often compiled over years of study, can have devastating effects. Natural or man-made disasters can destroy a database full of educational research, causing irrevocable damage unless a backup of that data exists. Geographically dispersed backups of research data ensure that, should one location be compromised, the research data is still secure. By utilizing a centralized management device, these backups can be instantaneously synchronized, with zero downtime.

PREPAID CARDS

The role of institution-issued cards within the realm of education has swelled over the past decade, providing universities with a means of increasing both the convenience and security of on-campus purchases. Many card issuance tasks are performed using a hardware security module.

Closed-loop prepaid cards, or merchant-specific cards, provide an ideal solution for universities seeking convenient payment options for on-campus dining, electronic printing services, and more. Providing students with a secure way to manage payments within the university infrastructure increases the opportunity and possibility of sales while better serving the university community.

Cards can be refilled or “topped off” with funds through on-campus kiosks or through online interfaces by parents or other third parties. Further, some institutions have begun a shift toward enhanced prepaid cards, allowing the same cards to be accepted at off-campus merchants. Such an increase in acceptance makes the university prepaid card more convenient for its users – and more useful and more widely used.

IDENTIFICATION CARDS

Physical security and access control plays a larger role on college campuses today than ever before, and an integral component of ensuring campus security is identification. Issuance of personalized identification cards can be used to limit building entry to only authorized individuals at specific times, admit students to their designated dormitories and rooms, and easily verify students’ identities at on and off-campus events.

These identification cards afford universities opportunities to increase the convenience of payments and security within their institutions. As with any enterprise that involves large-scale volumes of sensitive data, however, it is advisable to engage in a card issuance process that makes use of sophisticated, proven data security technology. Security, speed, regulatory compliance, and flexibility for future enhancement are four of the most important criteria that IT administrators in an education environment must take into consideration.

INSTITUTION-BASED TRANSACTIONS

Protecting cardholder data is an issue that spans across wide-ranging industries. For educational institutions, the process of paying for tuition, textbooks, on-campus eateries, and school or campus-sponsored events must be secure. PCI DSS governs the mandates required of institutions and merchants handling cardholder data, and the cost of non-compliance can be just as harsh as the cost of the data breach itself.

To maintain security of cardholder information before, during, and after a transaction, an HSM can facilitate encryption and secure storage. Utilizing tokenization enables customer information to be retained for purposes such as returns, refunds, or easy repeated purchases, all while avoiding the security risk of storing data in-the-clear.

HSMs meet all industry compliance standards and can significantly reduce the effort associated with maintaining compliance while enabling a more secure form of transaction processing and cardholder data storage.

FUTUREX SOLUTIONS FOR SECURING EDUCATIONAL INSTITUTIONS

The Futurex Hardened Enterprise Security Platform is a collection of advanced data security solutions that operate together to produce a result far beyond the sum of its parts. These solutions are custom-tailored by Futurex Solutions Architects to specific ecosystems and can be integrated directly with existing applications and business systems, enabling educational institutions to have complete, secure cryptographic systems.

The Hardened Enterprise Security Platform is available as physical units implemented at the academic institution's facility of choice, or it can be deployed in VirtuCrypt's secure cloud environment, with customizable functionality to meet the unique needs of educational institutions.

BEST-IN-CLASS HARDWARE SECURITY MODULES

Encryption and decryption tasks for educational institutions can be easily handled by Futurex's FIPS 140-2 Level 3 validated hardware security modules. These HSMs offer the fastest transaction processing speeds in the industry and are equipped with robust logical and physical security features to safeguard sensitive data.

HIGH AVAILABILITY INFRASTRUCTURES

Educational institutions may take holidays, but their core cryptographic infrastructures don't have that luxury. Because of this, the IT systems of educational institutions must support 99.999% uptime as well. As a cornerstone of the Hardened Enterprise Security Platform, the Guardian9000 provides centralized management, custom alerting, full redundancy, and N^{th} degree scalability for educational organizations' data security infrastructures.

CERTIFICATE AUTHORITY SOLUTIONS

Authentication of devices, application, files and other educational data lies at the heart of modern data security strategies. By creating mutually authenticated environments, educational organizations seek to secure their students and faculty's sensitive data. With Futurex's certificate authority solutions, schools and universities can issue certificates to sign and verify data for a variety of applications.

SYSTEM SCALABILITY AND STORAGE

Educational organizations are charged with managing large volumes of data ranging from student identifiable information to credit card numbers. The SAS9000 Secure Attached Server offers a high-volume, hardware-based data storage and access solution with full integration with other Futurex products. Sensitive information is encrypted and stored directly on the SAS9000's array of hot-swappable, RAID-enabled hard drives until the information needs to be accessed again.

SECURE SSL/TLS GATEWAY

As student information travels to and from storage locations, it poses an easy target for attackers. All communication must be secured, whether site-to-site or with endpoint devices like computers. Even networks protected behind a firewall are potentially at risk. The Kryptos TLS Server encrypts all connections, ensuring point-to-point encryption of all transmitted data when it is not housed within the secure confines of an encrypted database.

ENTERPRISE KEY MANAGEMENT SOLUTIONS

As educational institutions grow, so does their responsibility for key management. Futurex's enterprise series key management servers are FIPS 140-2 Level 3-validated solutions for managing the entire encryption key lifecycle including creation, management, distribution, and destruction for both symmetric and asymmetric keys in one central, secure location.

REMOTE CONFIGURATION AND MANAGEMENT

The Excrypt Touch, the world's only FIPS 140-2 Level 3-validated remote configuration and key loading tablet, adds the ability for systems administrators to manage and configure their entire cryptographic infrastructure remotely, performing tasks such as loading master keys and updating firmware from a remote location.

BENEFITS OF HARDWARE-BASED SECURITY

Schools and universities are epicenters of knowledge and information. The same knowledge that makes these institutions so valuable within society also makes them vulnerable targets for data breaches.

Encrypting and authenticating sensitive data within a hardware-based platform offers an unrivaled level of security. Hardware security modules implemented in educational IT infrastructures are purpose-built to protect student and faculty data using physical, logical, and encryption-based security features. Additionally, tamper resistance and responsiveness ensures active protection in the event of unauthorized access attempts.

Finally, HSMs can offer advanced disaster recovery and redundancy features – functions that maintain continued operation in the event of a disaster or unplanned outage, ensuring university research and academic records are always secure and available when needed.

Hardware-based encryption provides a secure, accessible means of protecting data and is currently required and implemented in a broad range of applications across multiple industries. Futurex maintains a global focus on speed, security, and service and is committed to assisting institutions of education in their data security efforts.

FUTUREX ENGINEERING CAMPUS
OFFICE: +1 830 - 980 - 9782 TOLL FREE: 800 - 251 - 5112
864 OLD BOERNE ROAD, BULVERDE, TEXAS, USA 78163